Naciones Unidas A/74/130

Asamblea General

Distr. general
30 de julio de 2019
Español
Original: inglés

Septuagésimo cuarto período de sesiones
Tema 109 del programa provisional*
Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos

Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos

Informe del Secretario General

Resumen

El presente informe se ha preparado en cumplimiento de la resolución 73/187 de la Asamblea General, titulada “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”. En esa resolución, la Asamblea General solicitó al Secretario General que recabara las opiniones de los Estados Miembros sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y que presentara un informe basado en esas opiniones para examinarlo en su septuagésimo cuarto período de sesiones.

El informe contiene información sobre las opiniones de los Estados Miembros presentadas en cumplimiento de la resolución mencionada.

* A/74/150.

V.19-08185 (S) 160919 160919

Índice

I. Introducción

1. En su resolución 73/187, titulada “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, la Asamblea General solicitó al Secretario General que recabara las opiniones de los Estados Miembros sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y que presentara un informe basado en esas opiniones para examinarlo en su septuagésimo cuarto período de sesiones.

2. En cumplimiento de esa solicitud, en las notas verbales CU 2019/55/DTA /OCB/CMLS y CU 2019/90/DTA/OCB/CSS, de 13 de febrero de 2019 y 19 de marzo de 2019 respectivamente, emitidas por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), la Secretaría invitó a los Estados Miembros a que presentaran información sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. La Secretaría comunicó a los Estados Miembros que la información se utilizaría para preparar el informe sobre la aplicación de la resolución 73/187, que se presentaría a la Asamblea General para que lo examinara en su septuagésimo cuarto período de sesiones. La Secretaría observó que las comunicaciones nacionales presentadas a los efectos del informe no debían exceder las 1.000 palabras, excluido el texto de las leyes o la legislación que cada Estado Miembro deseara presentar. Las leyes o la legislación presentadas de manera adjunta se publicarían en el portal de gestión de conocimientos para el intercambio de recursos electrónicos y legislación sobre delincuencia (SHERLOC).

3. En respuesta a la invitación, los siguientes Estados Miembros expresaron sus opiniones: Alemania, Arabia Saudita, Argentina, Armenia, Australia, Austria, Belarús, Bolivia (Estado Plurinacional de), Botswana, Brasil, Canadá, Chequia, China, Colombia, Costa Rica, El Salvador, Eslovaquia, Eslovenia, España, Estados Unidos de América, Estonia, Federación de Rusia, Filipinas, Francia, Georgia, Ghana, Hungría, India, Irán (República Islámica del), Iraq, Irlanda, Israel, Italia, Japón, Jordania, Líbano, Liechtenstein, Malasia, Marruecos, Mongolia, Myanmar, Nicaragua, Noruega, Nueva Zelandia, Países Bajos, Perú, Portugal, Qatar, Reino Unido de Gran Bretaña e Irlanda del Norte, República Árabe Siria, República Popular Democrática de Corea, Rumania, Serbia, Singapur, Sri Lanka, Sudáfrica, Suiza, Tailandia, Tayikistán, Turquía y Venezuela (República Bolivariana de).

4. Esas opiniones quedan reflejadas en los resúmenes preparados por la Secretaría, que se presentan a continuación. Las comunicaciones abarcaron los problemas en los planos nacional e internacional y las medidas adoptadas para hacerles frente en ambos planos, también en el marco de los mecanismos especializados existentes. Los Estados Miembros facilitaron información sobre los problemas técnicos y tecnológicos y compartieron sus experiencias relativas a la manera de hacerles frente. También destacaron la importancia de la cooperación internacional en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

II. Respuestas recibidas de los Gobiernos

Argentina

5. La Argentina consideró que entre los mayores desafíos a que se enfrentaban los Estados para contrarrestar la utilización de las tecnologías de la información y las comunicaciones con fines delictivos figuraban los siguientes:

a) El alcance de los instrumentos internacionales. Con excepción del Convenio sobre la Ciberdelincuencia, del Consejo de Europa, no se habían alcanzado aún otros acuerdos internacionales en la materia. La Argentina trabajaba activamente en las actividades del Comité del Convenio sobre la Ciberdelincuencia y recomendaba

a los Estados que aún no fueran partes que evaluaran adherirse a dicho instrumento a fin de fortalecer su aplicación y la adhesión de países que no fueran miembros del Consejo de Europa. No obstante, teniendo en cuenta la naturaleza global del fenómeno de la ciberdelincuencia y la necesidad de contar con mecanismos que permitieran responder a dicho fenómeno de manera global, la Argentina apoyaba tanto los procesos en el marco del Convenio del Consejo de Europa, como aquellas instancias de discusión que buscaban avanzar, en el marco de las Naciones Unidas, hacia la negociación de un marco jurídico universal en la materia;

b) Las dificultades para el acceso transfronterizo a las pruebas digitales. La principal dificultad en la mayoría de los casos se presentaba debido a que los datos que constituían la prueba se encontraban alojados en una jurisdicción distinta de aquella donde el delito era juzgado y, en casi todos los casos, en poder/control de empresas privadas. Las soluciones propuestas hasta el momento a esos problemas, como la Ley de los Estados Unidos por la que se Aclara el Uso Transfronterizo Lícito de Datos (vigente) y la iniciativa de la Unión Europea en materia de pruebas digitales (en trámite), no contemplaban acabadamente las necesidades de terceros países;

c) La insuficiente capacidad para medir los resultados en materia de intercambio de información y buenas prácticas. En muchos casos resultaba difícil mensurar los resultados en materia de intercambios de buenas prácticas y de información enunciados en los acuerdos;

d) Las dificultades en la actualización del marco normativo en relación con el avance tecnológico. Mantener actualizado el marco normativo penal, tanto de fondo como procesal, conllevaba muchas dificultades, que eran más graves en los países con sistemas legales codificados;

e) El bajo nivel de concientización en la población y en las organizaciones. Un aspecto esencial de la lucha contra el delito era el referido a la prevención. En el delito cibernético, la prevención se vinculaba directamente a la concientización, de las personas y las organizaciones, acerca de los riesgos y amenazas que entrañaba el uso de las tecnologías de la información y las comunicaciones. Era necesario formular planes nacionales de concientización bajo los cuales se articularan los esfuerzos e iniciativas, tanto privadas como públicas, de un modo que permitiera dotar de coherencia a los mismos y optimizara el uso de recursos;

f) La responsabilidad del sector privado. El sector privado desempeñaba un papel fundamental en relación con los desafíos que planteaba el delito cibernético. La responsabilidad de las empresas se verificaba en aspectos como el control y la gestión de las vulnerabilidades en materia de datos que presentaban las plataformas y los dispositivos, y el uso de las redes sociales con fines delictivos. Más allá de la cooperación voluntaria del sector privado, era preciso analizar la necesidad de reglas de cumplimiento obligatorio;

g) El crecimiento de los riesgos. La profusión del uso de dispositivos inteligentes de relativamente bajo costo que permitían el acceso a Internet sin un nivel mínimo de seguridad aumentaba la superficie de potenciales ataques y el alcance del delito cibernético. Para hacer frente a este crecimiento se requerían políticas de Estado y estrategias de responsabilidad corporativa complementarias. Los proyectos impulsados por algunos Estados para contar con mecanismos que les permitieran desencriptar información de dispositivos/aplicaciones o mecanismos de puerta trasera (*backdoors*) suponían un riesgo. También se habían de evaluar los instrumentos de penetración informática y extracción de información o monitoreo que proponían diversos cuerpos judiciales.

6. La Argentina había determinado que los principales desafíos que afrontaba en cuanto a la investigación y persecución de los delitos cometidos mediante el uso de las tecnologías de la información y las comunicaciones se referían a los siguientes puntos:

a) La capacitación de los operadores del sistema de justicia penal;

b) La necesidad de dotar de instrumentos de informática e investigación forenses adecuados al personal del poder judicial y de las fuerzas del orden;

c) La falta de definiciones en las leyes o de una tipificación adecuada de las conductas penales;

d) Normas procesales que tuvieran en cuenta las características especiales de las pruebas digitales;

e) La mejora de los mecanismos de cooperación internacional;

f) La mejora de la cooperación de las empresas del sector privado (proveedores de servicios de Internet).

7. La Argentina también afirmó que la capacitación en la esfera del delito cibernético y la recolección de pruebas digitales era el mayor desafío para lograr una persecución penal eficaz. Los esfuerzos debían estar enfocados en ampliar los conocimientos de los operadores del sistema y así lograr una mejor aplicación de las leyes e instrumentos internacionales vigentes. Ello aseguraría no solo una respuesta efectiva contra esos delitos, sino también el respeto por los derechos fundamentales de las partes del proceso.

8. La Argentina valoraba los aportes hechos por las organizaciones internacionales y regionales, como las Naciones Unidas (por conducto de la UNODC), la Organización de los Estados Americanos, la Unión Europea y el Consejo de Europa, para compartir mejores prácticas y experiencias. El Ministerio de Justicia trabajaba actualmente en la elaboración de normas procesales modelo para la obtención de pruebas digitales que sirvieran de base tanto a la legislación federal como a la provincial.

9. La Argentina era un país federal, lo cual implicaba que coexistía un sistema de justicia federal junto con 24 sistemas de justicia provinciales. Ello dificultaba la respuesta ante fenómenos complejos e internacionales como el delito cibernético y las pruebas digitales. Una práctica de gran utilidad que se había implementado era la creación de unidades fiscales especializadas. La Argentina trabajaba para que las distintas jurisdicciones adoptaran ese modelo y agilizaran las investigaciones y el intercambio de información.

10. La Argentina también dio a conocer el desafío adicional que planteaba la insuficiencia de recursos financieros para afrontar las transformaciones necesarias, tanto en el poder judicial como en las fuerzas de seguridad, el cual implicaba esfuerzos sostenidos expresados como una política de Estado.

Armenia

11. Armenia afirmó que los órganos estatales y organismos gubernamentales pertinentes estaban adoptando constantemente medidas para afrontar los cambiantes riesgos derivados de la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y, en ese sentido, mejorar la legislación sectorial, por ejemplo, mediante un continuo diálogo con las entidades especializadas de las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa, la Unión Europea y el Consejo de Europa, así como mediante una mayor cooperación e intercambio de información en el marco del Centro contra el Terrorismo de la Comunidad de Estados Independientes, la Organización del Tratado de Seguridad Colectiva y la Organización Internacional de Policía Criminal (INTERPOL).

12. Armenia comunicó que, para el período 2019–2020, tenía previsto establecer un grupo de trabajo interinstitucional que se encargara de formular conceptos, planes de acción y estrategias nacionales en las esferas de la información y la ciberseguridad. El grupo de trabajo estaría integrado por funcionarios públicos y expertos, instituciones científicas y de investigación, fundaciones y organizaciones de la sociedad civil y del sector privado, según procediera.

13. Armenia también comunicó que se habían redactado los proyectos de ley sobre la modificación del Código Penal y el Código de Procedimiento Penal, respectivamente, cuya aprobación estaba prevista dentro de un futuro próximo. En ese conjunto de proyectos de ley se disponían modificaciones y adiciones a los artículos relativos a los delitos cometidos con el uso de sistemas informáticos. Durante el proceso de redacción

del proyecto de Código de Procedimiento Penal, se habían celebrado diversas reuniones con representantes de los expertos policiales del Consejo de Europa.

14. Armenia llevaba a cabo evaluaciones periódicas de los riesgos nacionales en materia de blanqueo de dinero y financiación del terrorismo. En 2017 se llevó a cabo la evaluación más reciente del período 2014–2017. La actualización analítica del Informe de Evaluación Nacional de los Riesgos de Blanqueo de Dinero y Financiación del Terrorismo publicado en 2014[1] reveló ciertos riesgos en materia de blanqueo de dinero vinculados con la utilización de las tecnologías de la información y las comunicaciones. Se constató que, cada vez más, se estaban utilizando nuevos productos y mecanismos de entrega de dinero (por ejemplo, terminales punto de venta en línea, banca electrónica y móvil, y monederos electrónicos) para entablar relaciones comerciales o efectuar transacciones complejas y de una magnitud inusitada.

15. Armenia señaló que los productos y servicios que utilizaban terminales punto de venta y sistemas de banca electrónica presentaban flaquezas a efectos de determinar los riesgos que podrían plantearse durante las relaciones comerciales. En particular, una vez establecida una relación comercial con un cliente y adoptadas las medidas iniciales necesarias de diligencia debida con respecto a este, la actividad comercial posterior del cliente se producía en un entorno en línea, sin que hubiera un contacto cara a cara con el personal bancario pertinente (dirección). En esa clase de relaciones había menos oportunidades para detectar actividades sospechosas. Además, los datos robados de tarjetas emitidas por bancos extranjeros podían utilizarse para registrar cuentas de monederos electrónicos, que se activaban introduciendo un conjunto de elementos identificadores válidos de la tarjeta (número, fecha de caducidad, valor de verificación de tarjeta (CVV)). Los perpetradores podrían, por lo tanto, acceder a servicios financieros sin pasar por los procedimientos obligatorios de diligencia debida con respecto al cliente. Los monederos electrónicos registrados podían, posteriormente, utilizarse para realizar numerosas transferencias electrónicas a fin de ocultar el origen del producto del delito, con la subsiguiente transferencia de los saldos disponibles en las cuentas.

16. Teniendo en cuenta los factores de riesgo detectados, el Centro de Fiscalización Financiera del Banco Central de Armenia había venido adoptando las medidas pertinentes para su prevención y disuasión, y para ello había transmitido, por ejemplo, encargos e instrucciones pertinentes a determinadas instituciones financieras.

17. En 2018 la División de Lucha contra la Delincuencia de Alta Tecnología de la Dirección General de Lucha contra la Delincuencia Organizada de la policía había iniciado 79 causas penales. De ellas, 70 guardaban relación con la delincuencia de alta tecnología y las 9 restantes, que se habían iniciado con arreglo a lo dispuesto en otros artículos, estaban estrechamente vinculadas con la utilización de las tecnologías de la información y las comunicaciones.

18. Conforme a las conclusiones de un estudio realizado por la policía, habían aumentado las actuaciones penales sobre la base de los artículos 181 (Robo cometido mediante computadora) y 254 (Apropiación ilícita de datos informáticos) del Código Penal de Armenia. En el estudio se sugirió que tanto las personas físicas como las jurídicas eran susceptibles de ser víctimas de los actos recogidos en el artículo 181, mientras que las víctimas de los delitos comprendidos en el artículo 254 eran en su mayoría usuarios de las redes sociales o de servicios de correo electrónico. La divulgación de esos delitos obedecía sobre todo a que se hubieran cometido en el extranjero o a que hubieran quedado ocultos rastros del delito en los sistemas de

[1] En la Evaluación Nacional de los Riesgos de Blanqueo de Dinero y Financiación del Terrorismo se examinaban las amenazas y vulnerabilidades en los sectores en que se observaban avances significativos y respecto de los cuales los expertos formulaban recomendaciones como parte de la evaluación mutua del sistema que existía en Armenia para combatir el blanqueo de dinero y la financiación del terrorismo, a cargo del Comité de Expertos sobre Evaluación de Medidas contra el Blanqueo de Dinero y la Financiación del Terrorismo del Consejo de Europa. El resumen podía consultarse en www.cba.am/Storage/EN/FDK/risk_assesment/NRA_Update_Executive_Summary(Public)_eng.pdf.

servidores de varios países. En esos casos, por consiguiente, las investigaciones se complicaban debido a las diferencias en la legislación de los distintos países. Como resultado de ello, la información no solía llegar hasta el organismo encargado de hacer cumplir la ley que la solicitaba.

19. De conformidad con las disposiciones pertinentes del Convenio sobre la Ciberdelincuencia del Consejo de Europa, el punto de contacto nacional dentro de la policía había adoptado medidas para detectar a los usuarios de las redes sociales ajenas a la Federación de Rusia y revelar su identidad. Se habían formulado solicitudes de información relativas a las operaciones o a las causas penales a través de la red de puntos de contacto 24 horas. Según informó Armenia, la subdivisión especializada[2] prestaba asistencia y asesoramiento profesionales respecto de cuestiones sectoriales a las subdivisiones territoriales de la policía, previa solicitud (oral o por escrito). Además, se había organizado un curso de capacitación en el que habían participado los jefes de las subdivisiones territoriales de policía y durante el cual se habían explicado en detalle las características de los delitos informáticos y el proceso de recabar pruebas.

20. Los funcionarios de las subdivisiones especializadas de la policía habían visitado las organizaciones internacionales pertinentes y habían asistido a talleres y seminarios adaptados a sus necesidades para estudiar las mejores prácticas en la lucha contra la ciberdelincuencia[3]. En Armenia se habían llevado a cabo los arreglos organizativos pertinentes dentro del marco de la Operación Proxy de la Organización del Tratado de Seguridad Colectiva, que tenía por objeto combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. La policía venía realizando actividades destinadas a concienciar respecto de las cuestiones y los problemas relacionados con las tecnologías de la información y las comunicaciones[4].

21. La subdivisión especializada de la policía había estado vigilando la zona de dominio armenio y el segmento armenio de las redes sociales populares, a fin de detectar delitos. La vigilancia no se limitaba a la detección de ciberdelincuencia (por ejemplo, programas secuestradores), sino que también comprendía los actos delictivos (como chantaje, extorsión y suicidio forzado) en los que Internet servía únicamente como medio para cometer un delito y no como instrumento directo.

22. Armenia afirmó también que, desde el punto de vista de la seguridad de la información, la instigación de actos de intolerancia, violencia, odio, xenofobia y prácticas extremistas y terroristas basados en la identidad, así como la glorificación de los autores de actos genocidas mediante el uso de Internet, especialmente en caso de ser alentados y orquestados a nivel estatal, eran motivo de grave preocupación y entrañaban el riesgo de que las sociedades se radicalizaran y de que surgieran combatientes terroristas extranjeros. Al mismo tiempo, Armenia hizo hincapié en que los derechos humanos y las libertades fundamentales, incluidos los derechos colectivos, deberían garantizarse de manera igualitaria e indiscriminada tanto en línea como fuera de línea, independientemente de las fronteras[5] y de la condición jurídica de los territorios.

[2] La subdivisión especializada realizaba, en cumplimiento de la ley pertinente, actividades operacionales de búsqueda a partir de las tareas encomendadas dentro del marco de las causas penales, y tramitaba las solicitudes recibidas de los ciudadanos.

[3] En concreto, durante un acto organizado conjuntamente por la Unión Europea y el Consejo de Europa, se habían presentado métodos avanzados de lucha contra la ciberdelincuencia dentro del marco de los proyectos Facility 2 (Refuerzo de la reforma judicial) y Facility 3 (Medidas de apoyo contra las formas graves de ciberdelincuencia) de la Asociación Oriental. Asimismo, se habían examinado el proyecto de Código de Procedimiento Penal, las perspectivas de las reformas legislativas y los fundamentos jurídicos para la cooperación con el sector privado.

[4] Entre las actividades figuraron entrevistas a diversos medios de comunicación, la participación en conferencias de prensa, la emisión de una amplia gama de material de información pública y contribuciones a programas de televisión.

[5] Conforme a lo establecido y mencionado implícitamente en el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos.

Australia

23. Australia consideraba que la ciberdelincuencia comprendía delitos dirigidos a computadoras y delitos más tradicionales facilitados por el uso de computadoras. Además, subrayó la necesidad de centrar los debates en los conocimientos técnicos especializados existentes. Los desafíos que planteaba la ciberdelincuencia eran complejos y cambiantes. Para hacerles frente se necesitaban una atención constante y la orientación y el asesoramiento de expertos técnicos en ciberdelincuencia. En este contexto, Australia valoraba en gran medida la labor del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, establecido de conformidad con la resolución 65/230 de la Asamblea General. Australia consideraba que el Grupo de Expertos, en la medida en que en él recaía el mandato de las Naciones Unidas en materia de intercambios sobre ciberdelincuencia, debería mantenerse como foro principal para las deliberaciones al respecto. En términos más amplios, la UNODC ostentaba el mandato pertinente de las Naciones Unidas de luchar contra la delincuencia transnacional y las drogas. Dado que la ciberdelincuencia era un delito transnacional, convenía que las deliberaciones al respecto siguieran manteniéndose principalmente en Viena y bajo los auspicios de la UNODC. Australia aguardaba con interés el informe que el Grupo de Expertos presentaría en 2021, incluidas sus conclusiones y recomendaciones sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional.

24. Por lo que respectaba a los datos extraterritoriales, y al igual que todos los Estados Miembros, Australia comunicó que sus organismos nacionales encargados de hacer cumplir la ley se enfrentaban a dificultades para obtener datos y acceder a ellos a fin de investigar y perseguir la ciberdelincuencia de manera eficaz. Antaño, los datos solían almacenarse en territorio nacional y podían consultarse utilizando las competencias investigadoras nacionales. En la actualidad, dada la creciente conectividad mundial y la dependencia cada vez mayor respecto de la computación en la nube, los datos se distribuían por distintos servidores, proveedores, ubicaciones y jurisdicciones. Esos datos podían ser difíciles de localizar y podían obtenerse únicamente mediante complejos y lentos procesos de cooperación jurídica internacional. El uso cada vez mayor de los servicios de comunicaciones OTT se traducía en que las competencias tradicionales de las órdenes judiciales para acceder a las comunicaciones alojadas en portadores y proveedores de servicios portadores no capturaban la amplitud de datos necesaria para las investigaciones en materia de ciberdelincuencia.

25. Australia recalcó que las soluciones ofrecidas por los tratados, como el Convenio sobre la Ciberdelincuencia del Consejo de Europa, brindaban una base establecida para permitir el acceso de los organismos encargados de hacer cumplir la ley a los datos ubicados en otro Estado cuando, por ejemplo, la persona con autoridad legítima manifestaba su consentimiento para revelar los datos o cuando la información era de acceso público. Las restricciones que fueran más allá de esas circunstancias, como exigir el consentimiento de las autoridades estatales, planteaban importantes problemas para la investigación y persecución de la ciberdelincuencia.

26. Los mecanismos tradicionales de cooperación jurídica internacional, como la asistencia judicial recíproca, a duras penas conseguían mantener el ritmo de la demanda, y eso causaba demoras en las investigaciones de delitos cibernéticos. Otros marcos de cooperación internacional entre las autoridades competentes, las autoridades encargadas de hacer cumplir la ley y, cuando procediera y en consonancia con el derecho interno, los proveedores de servicios de comunicaciones de los Estados, podían brindar soluciones prácticas y expeditas.

27. Australia informó de que utilizaba satisfactoriamente tratados multilaterales, por ejemplo, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia del Consejo de Europa, como base para la cooperación jurídica internacional, además de sus arreglos bilaterales y nacionales. Los nuevos mecanismos, como los que se contemplaban en el protocolo adicional en proceso de negociación (relativo al acceso transfronterizo a los datos) al Convenio sobre la Ciberdelincuencia del Consejo de Europa, respondían a la

naturaleza cambiante de la ciberdelincuencia y mejorarían sustancialmente la capacidad que los organismos encargados de hacer cumplir la ley tenían para acceder a los datos de cara a las investigaciones sobre ciberdelincuencia. Al permitir un acceso más eficiente a los datos, era posible lograr un equilibrio entre los objetivos de cumplimiento de la ley y los de protección de datos.

28. Desde el punto de vista de las salvaguardias y las facultades policiales, Australia señaló que hacían falta mecanismos de vigilancia apropiados a fin de equilibrar la salvaguardia de los derechos humanos y de las libertades fundamentales con la necesidad legítima que las entidades encargadas de hacer cumplir la ley tenían de ejercer sus competencias de investigación para combatir la ciberdelincuencia. En Australia, las autoridades encargadas de hacer cumplir la ley estaban sujetas a una vigilancia considerable, sobre todo en el ejercicio de facultades más intrusivas, como el acceso a contenido de comunicaciones almacenado y la interceptación en tiempo real. Algunas de esas salvaguardias eran la necesidad de que la autoridad judicial ejerciera sus facultades, requisitos parlamentarios en materia de presentación de informes, el derecho de los imputados a impugnar la admisibilidad de las pruebas y el derecho de interponer un recurso, así como la vigilancia de toda orden judicial en materia de telecomunicaciones por parte del *ombudsman* del Commonwealth. Velar por que las facultades policiales estuvieran debidamente equilibradas con las salvaguardias exigía una evaluación continua y un examen constante, lo cual podía plantear un reto en algunas jurisdicciones.

29. Con respecto a la cuestión de la adaptabilidad de los marcos jurídicos y operacionales, Australia recalcó su compromiso de mantener los marcos legislativos nacionales adaptables que siguieran el ritmo del rápido avance tecnológico y conductual. Australia reconoció el desafío que planteaba redactar leyes que abarcaran los delitos cibernéticos sustantivos, las facultades procesales en las investigaciones sobre ciberdelincuencia y la admisibilidad de las pruebas electrónicas, sin dejar de ser aplicables a las cambiantes tecnologías y comportamientos. A fin de hacer frente a ese desafío, Australia promovía, en el plano nacional y como parte de sus iniciativas de creación de capacidad, una legislación tecnológicamente neutra en la que se tuvieran en cuenta los comportamientos y tecnologías futuros en materia de ciberdelincuencia.

30. Australia informó de que su legislación y sus reglamentos se basaban en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, que era el principal instrumento internacional sobre ciberdelincuencia y brindaba un sólido fundamento jurídico y operacional para la cooperación internacional contra la ciberdelincuencia. El Convenio contaba con 63 Estados partes, de los cuales más de la mitad no eran miembros de la Unión Europea. Australia comunicó que, en su experiencia, el Convenio era moderno y progresista y estaba deliberadamente dotado de neutralidad tecnológica, lo cual le permitía evolucionar y mantener su pertinencia conforme iban apareciendo nuevas tecnologías. Asimismo, había sentado las bases de los enfoques legislativos nacionales en regiones de todo el mundo, también en países que en ese momento no eran partes en el Convenio.

31. Australia también opinaba que, además de amplios marcos para la tipificación de la ciberdelincuencia, hacía falta una capacitación sostenible y continua para los funcionarios encargados de hacer cumplir la ley que trabajaban en primera línea. En la capacitación deberían tratarse los temas de la delincuencia facilitada por la tecnología y la recopilación y el uso de pruebas digitales. Australia consideraba importante mantener y brindar una capacitación actualizada y sostenible a las entidades encargadas de hacer cumplir la ley en el país, así como a asociados internacionales, mediante programas de creación de capacidad.

32. La ciberdelincuencia exigía, dada su naturaleza, una estrecha cooperación con otros Estados. Australia se había encontrado con dificultades cuando los Estados con los que debía cooperar en materia de ciberdelincuencia tenían una capacidad limitada o carecían de ordenamientos jurídicos amplios para hacer frente a la ciberdelincuencia. Para resolver ese problema era necesario que los Estados se centraran en crear y reforzar la capacidad de lucha contra la ciberdelincuencia, por ejemplo, mediante capacitación especializada al respecto. Australia subrayó que la prestación de asistencia para la

reforma legislativa también era importante para los países en desarrollo. Australia brindaba creación de capacidad y asistencia técnica a los Estados para ayudarles a fomentar su capacidad técnica. Asimismo, apoyaba la valiosa labor del Programa Mundial contra el Delito Cibernético, de la UNODC.

Austria

33. Al informar acerca de los desafíos mundiales en la lucha contra la ciberdelincuencia, Austria afirmó que la ciberdelincuencia era un problema cambiante que afectaba a todos los países y que exigía un enfoque eficiente y eficaz a fin de:

a) Aumentar al máximo el número de países que contaran con una legislación nacional adecuada y compatible en materia de ciberdelincuencia, en la que también se apoyara la cooperación internacional;

b) Crear mecanismos de cooperación, confianza y competencias para compartir datos con objeto de investigar, perseguir y reducir la ciberdelincuencia.

Esto incluía, entre otras cosas, velar por que no existieran lugares seguros para los autores de delitos cibernéticos y fortalecer la capacidad de los funcionarios encargados de hacer cumplir la ley y de las autoridades judiciales para investigar, enjuiciar y condenar eficazmente a los ciberdelincuentes.

34. A fin de garantizar una amplia legislación cibernética en toda la Unión Europea, sus Estados miembros, entre ellos Austria, habían convenido un conjunto de instrumentos que proporcionaban definiciones comunes de los delitos: una directiva relativa a los ataques contra los sistemas de información, una directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, y la Decisión Marco de 28 de mayo de 2001 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo[6]. Además, el 17 de abril de 2018, la Comisión Europea había presentado propuestas legislativas para mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones penales.

35. Sin embargo, el acceso a las pruebas electrónicas solo podía verse como un primer paso, pues faltaba un plan común para la conservación de datos a nivel europeo que salvaguardara la disponibilidad de pruebas electrónicas. Por eso, el plazo y la cantidad de pruebas electrónicas variaban enormemente entre los distintos Estados miembros de la Unión Europea y podían incluso depender de la buena voluntad de las organizaciones. En ese contexto, la problemática situación en materia de WHOIS, respecto de la cual no había aún una solución operativa, resultaba pertinente. La necesidad de mejorar el acceso a las pruebas electrónicas se trataría en un segundo protocolo al Convenio sobre la Ciberdelincuencia del Consejo de Europa.

36. Austria señaló que, en 2013, la Agencia de la Unión Europea para la Cooperación Policial (Europol) había establecido el Centro Europeo contra la Ciberdelincuencia (EC3), que había contribuido notablemente a los esfuerzos de los Estados miembros de la Unión Europea para combatir la ciberdelincuencia utilizando un ágil modelo de lucha contra el delito. Austria declaró que era necesario lograr la participación de los fiscales en la fase más temprana posible de los casos de ciberdelincuencia, y consideró beneficioso el establecimiento de redes especializadas como la Red Judicial Europea sobre Ciberdelincuencia.

37. En relación con las opciones para fortalecer las respuestas actuales y proponer nuevas respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional, Austria señaló que la ciberdelincuencia era un problema mundial; toda nación necesitaba la asistencia de otros países para combatirla. Austria consideró que el Convenio sobre la Ciberdelincuencia del Consejo de Europa representaba un

[6] La Decisión Marco ya no está en vigor. Al 29 de mayo de 2019, fue sustituida por la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo (*Diario Oficial de la Unión Europea*, L 123, 10 de mayo de 2019), págs. 18 a 29.

modelo para las legislaciones nacionales y un valioso marco para la cooperación internacional y brindaba un instrumento flexible de elección incluso para los países que no eran miembros del Consejo de Europa. Por lo tanto, Austria no secundó los llamamientos a favor de la elaboración de un nuevo instrumento internacional sobre la ciberdelincuencia.

38. Austria afirmó que el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético era y debería seguir siendo el principal proceso a nivel de las Naciones Unidas en materia de ciberdelincuencia, al menos hasta 2021. El Grupo de Expertos había dado resultados, por ejemplo, con respecto a las reformas legislativas basadas en las normas internacionales vigentes y, en particular, por lo que se refería a la creación de capacidad. Debería realizarse una actualización del proyecto de estudio exhaustivo sobre el delito cibernético presentado en 2013, y para ello se necesitarían los conocimientos técnicos del Grupo de Expertos.

39. Austria sugirió que la UNODC y los Estados Miembros cumplieran esos objetivos y que los Estados Miembros prestaran apoyo a la UNODC para centrarse en las esferas concretas en las que pudiera influir realmente en la lucha contra la amenaza de la ciberdelincuencia, de la siguiente manera:

a) Reforzando las competencias policiales y de aplicación de la ley respecto de la capacitación general y especializada;

b) Creando asistencia técnica en los países en desarrollo;

c) Realizando un análisis de las deficiencias en la cooperación internacional a fin de determinar las esferas prioritarias;

d) Prestando apoyo a campañas de sensibilización pública para reforzar la prevención del delito y para lograr que la sociedad civil y las empresas cooperaran con las entidades encargadas de hacer cumplir la ley;

e) Fortaleciendo los mecanismos operacionales existentes, como la Red 24/7;

f) Recopilando datos sobre las amenazas que planteaba la ciberdelincuencia;

g) Actuando como un repositorio de mejores prácticas y estudios de casos respecto de la lucha contra el delito cibernético.

Belarús

40. Teniendo en cuenta la modernización de la narcodelincuencia moderna y la utilización de la Internet oscura y las criptomonedas para el tráfico de drogas, Belarús creía que una de las prioridades de los Estados Miembros debería ser velar por el intercambio de información, a escala supranacional, respecto de los medios para cometer delitos y los métodos de detección de actividades delictivas en la Internet oscura; la reunión e incautación de pruebas electrónicas; y el desarrollo y uso de técnicas específicas en la investigación de los delitos cometidos en el espacio virtual. Uno de los medios para combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos podía ser la capacitación de los funcionarios encargados de hacer cumplir la ley con respecto a cómo funcionaban la Internet oscura y las criptoindustrias. Belarús destacó que era importante elaborar un mecanismo jurídico internacional (recomendaciones) sobre el procedimiento de incautación de los criptoactivos ilícitos y de su almacenamiento hasta que el tribunal dictara sentencia.

41. Belarús señaló que la Política de Seguridad de la Información se había aprobado el 18 de marzo de 2019. En ella se habían dispuesto tareas y prioridades estratégicas en la esfera de la seguridad de la información y la lucha contra la ciberdelincuencia. La Política se basaba en los intereses geopolíticos de Belarús y en los acuerdos internacionales de cooperación en la esfera de la seguridad de la información internacional, teniendo en cuenta las disposiciones principales de las resoluciones de la Asamblea General, así como las recomendaciones formuladas por la Organización para la Seguridad y la Cooperación en Europa.

42. Belarús consideró que la elaboración y aprobación de un instrumento internacional universal dentro del marco de las Naciones Unidas facilitaría una mayor cooperación entre los órganos competentes de los Estados Miembros en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

Bolivia (Estado Plurinacional de)

43. El Estado Plurinacional de Bolivia señaló que el avance de la tecnología había repercutido en todos los aspectos de la actividad humana tanto dentro del país como en todo el mundo, así como en la seguridad en relación con el uso de nuevas tecnologías. Las tecnologías de la información y las comunicaciones habían permitido que los delitos tradicionales evolucionaran y se extendieran a través del uso de *software*, aplicaciones y redes de comunicación. La dependencia digital que tenían las entidades financieras había facilitado la comisión de delitos como el fraude. Asimismo, la fácil accesibilidad a números celulares sin registro personal había propiciado el anonimato en la comisión de delitos.

44. Para la Policía Boliviana, prevenir el delito y garantizar la seguridad en las comunicaciones eran grandes prioridades. Dentro de la Fuerza Especial de Lucha contra el Crimen se había creado la División Cibercrimen, una dependencia especializada para detectar delitos cometidos mediante las tecnologías de la información y las comunicaciones. La entidad nacional del orden contaba con unidades de monitoreo de prensa y redes sociales. El monitoreo de las redes sociales buscaba evitar las "burbujas informativas" (que limitaban la información a fin de incidir negativamente en la opinión pública) y prevenir extorsiones, amenazas, trata de personas, estafas, ciberacoso, discriminación y otros delitos que atentan contra la seguridad del Estado.

45. El Estado Plurinacional de Bolivia comunicó que los niños, en particular, los jóvenes de 12 a 18 años, estaban sometidos a los riesgos relacionados con la utilización de las tecnologías de la información y las comunicaciones, al verse expuestos a esas nuevas tecnologías desde una edad temprana y al utilizarlas regularmente para satisfacer sus necesidades de entretenimiento, diversión, comunicación e información. Sin embargo, no siempre obtenían un beneficio pedagógico o educativo de esas tecnologías.

46. El Estado Plurinacional de Bolivia brindó la siguiente lista no exhaustiva de formas de mal uso de las tecnologías de la información y las comunicaciones y de delincuencia informática:

a) Acoso, injurias, calumnias, hostigamiento y exclusión social a través de las redes sociales, del uso de correos electrónicos e, incluso, de los espacios de comentarios en las secciones de opinión de los diarios. En contextos aparentemente inofensivos, como en los colegios, se generaban campañas anónimas contra determinados niños a través, por ejemplo, de Facebook; se calumniaba a estudiantes universitarias, por ejemplo, acusándolas de prostitución; y se intentaba desacreditar a empresas determinadas a partir de hechos falsos;

b) Estafas y fraudes, entre ellos el *phishing*, mediante el cual las organizaciones delictivas se apropiaban de información confidencial que les permitía acceder a cuentas bancarias y desocuparlas. Otro ejemplo eran las campañas en línea de reclutamiento de gente para empleos, que actuaban como tapadera de redes involucradas en la trata de personas y la pornografía infantil. En general, el fraude se relacionaba con el acceso a información confidencial, así como con la posibilidad de alteración de la misma;

c) Correos basura. Aunque no necesariamente constituyeran una infracción de la ley, eran el resultado del uso indebido de bases de datos con fines comerciales que muchas empresas utilizaban para extender sus campañas de mercadeo a los potenciales usuarios. Se incluían campañas de prostitución y otras con fines ilícitos;

d) Pornografía infantil. Había grupos delictivos que, en forma de fotos y vídeos, la comercializaban a través de la red. Esto entrañaba una vulneración de la Convención sobre los Derechos del Niño y el Código Penal;

e) Propiedad intelectual. Los derechos de personas y organizaciones innovadoras se vulneraban de múltiples formas, incluyendo el “fusilamiento” (es decir, la toma de fotos) de textos protegidos (derechos de autor);

f) Ventas en Internet, como supuestos intermediarios de loterías y concursos.

47. El Estado Plurinacional de Bolivia afirmó que, a la par del desarrollo tecnológico informático, los delincuentes encontraban formas innovadoras de cometer fraudes y otros delitos que iban más rápido que los códigos penales. Frente a un fenómeno en alza, se imponía la necesidad de prevención y protección, que era deber de todos: Estado, empresas, organizaciones, ciudadanía. En este sentido, las innovaciones tecnológicas planteaban múltiples desafíos para las instituciones encargadas de mantenerlas:

a) La falta de conciencia y conocimiento por parte de la población respecto del uso de las tecnologías de la información y las comunicaciones. Esa carencia hacía que las personas fueran más vulnerables a delitos de diferente índole. Un desafío conexo sería cómo elaborar políticas adecuadas para mejorar los conocimientos acerca del buen uso de esas tecnologías;

b) La existencia de un vacío legal producto del desconocimiento o de la inaplicabilidad de las legislaciones actuales a los nuevos delitos para cuya comisión se utilizaban las tecnologías de la información y las comunicaciones. Era necesario, por lo tanto, revisar y actualizar la legislación;

c) La necesidad de modificar las estrategias de investigación y respuestas tradicionales a los delitos mediante la utilización de nuevos métodos, habida cuenta de la evolución de los delitos en los que se emplean las tecnologías de la información y las comunicaciones;

d) La necesidad de ser parte en convenios internacionales de cooperación sobre investigación, aseguramiento y obtención de pruebas en materia de ciberdelincuencia. Varios países de América Latina formaban parte ya de convenios y habían progresado en el desarrollo de sus capacidades tecnológicas en la prevención e investigación de delitos cometidos a través de las tecnologías de la información y las comunicaciones.

48. El Estado Plurinacional de Bolivia recordó que la incorporación de nuevas tecnologías en las instituciones gubernamentales repercutía en la cultura organizativa de cualquier institución, modificando los procedimientos e incorporando nuevos conocimientos asimilados. Muchas de las tecnologías desarrolladas e implementadas en las instituciones de seguridad requerían conocimientos específicos, lo que debía llevar a una apertura de las instituciones a trabajar con personas u organismos que no necesariamente pertenecían al área de seguridad, como universidades, institutos técnicos, centros de investigación y proveedores de *software*. En la actualidad, tanto policías como ciudadanos disponían de diversas herramientas tecnológicas para hacer frente a problemas de seguridad y actos delictivos, en algunos casos en la prevención de delitos y, en otros, como ayuda frente a la investigación de estos. Algunos de estos elementos se encontraban bastante difundidos, tanto a nivel de ciudadanía como de policías, mientras que otros eran de acceso más caro y difícil para el público en general.

49. Como conclusión, el Estado Plurinacional de Bolivia afirmó que los avances tecnológicos habían permitido la generación de nuevas dinámicas delictivas, lo que había obligado a las instituciones a adaptarse e incorporar estrategias innovadoras que les permitieran estar un paso por delante de los delincuentes, defendiendo la sociedad y manteniendo el orden público mediante la prevención e investigación de los delitos. Por lo tanto, era inconcebible para las instituciones encargadas de la seguridad pensar en hacer frente al fenómeno delictivo sin el uso de herramientas tecnológicas. Las instituciones responsables de la seguridad podrían no solo hacer uso de las herramientas tecnológicas internamente, sino que también podrían utilizarlas para involucrar a la ciudadanía en la prevención del delito.

Botswana

50. Botswana señaló las siguientes dificultades en la lucha contra la delincuencia, especialmente respecto de los delitos facilitados por la utilización de las tecnologías de la información y las comunicaciones:

a) La falta de armonía en la legislación en materia de ciberdelincuencia y protección de datos entre los diversos países y jurisdicciones dificultaba en gran medida la investigación de las actividades delictivas en el ciberespacio;

b) La falta de un marco internacional para el intercambio de información sobre ciberseguridad entre los diversos organismos de distintos países resultaba ser un desafío para la protección de las redes y la investigación de las actividades delictivas que abarcaban varias jurisdicciones;

c) La aparición de nuevas innovaciones tecnológicas, como la inteligencia artificial y la Internet de las cosas, que podrían aplicarse a esferas como las aplicaciones agrícolas, las aplicaciones médicas y el análisis de datos climáticos, pero que también brindaban una plataforma a partir de la cual, o mediante la cual, se podrían producir ciberataques;

d) Otro gran obstáculo o desafío es el que planteaba el fomento de la capacidad entre los diversos actores, es decir, los organismos encargados de hacer cumplir la ley, los proveedores de servicios, los encargados de la formulación de políticas y las entidades reguladoras, a fin de hacer frente a cuestiones en materia de ciberseguridad;

e) Dificultades para hacer frente a las empresas multinacionales que ofrecían servicios en el mercado nacional mientras carecían de licencia, como Facebook, WhatsApp, Google, Microsoft y Netflix. El proceso para obtener información o pruebas relativas a los delitos cometidos mediante sus redes era complicado;

f) Botswana y muchos otros países no eran partes en los tratados vigentes en materia de tecnologías de la información y las comunicaciones y de ciberseguridad (por ejemplo, la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales y el Convenio sobre la Ciberdelincuencia del Consejo de Europa), y esto hacía que fuera difícil recurrir amparándose en ellos. El Convenio sobre la Ciberdelincuencia ofrecía un marco jurídico para la cooperación internacional en materia de ciberdelincuencia y pruebas electrónicas, y se debería alentar a los países a que se hicieran partes en él;

g) Los procesos de asistencia judicial recíproca eran lentos y engorrosos, y eso hacía que en Botswana y otros países la justicia fuera ineficiente;

h) El carácter voluntario de la divulgación en materia de ciberdelincuencia seguía siendo un obstáculo en muchas jurisdicciones. El proceso de obtención de información era largo y en algunos casos imposible; esto obedecía en parte a que las normas para acceder a la información de los abonados diferían de un país a otro. Un acto que Botswana pudiera interpretar o considerar como delito podría no serlo en otro Estado.

51. Botswana formuló las siguientes recomendaciones:

a) Se necesitaban la cooperación y la colaboración de organismos como la UNODC, la Unión Internacional de Telecomunicaciones e INTERPOL, para que trabajaran conjuntamente a fin de resolver los problemas que planteaban los delincuentes que utilizaban redes digitales y tecnológicas para cometer delitos. Habían de aclararse las funciones de los distintos organismos en materia de ciberseguridad;

b) Debería elaborarse un marco internacional para que los Estados Miembros de las Naciones Unidas intercambiaran información relativa a la ciberseguridad;

c) Era necesario contar con un marco reglamentario y de políticas internacional que se ocupara de la utilización adecuada de las nuevas tecnologías, como la inteligencia artificial y la Internet de las cosas;

d) Deberían crearse programas de fomento de la capacidad para los Estados Miembros;

e) Debería elaborarse un marco para que las empresas multinacionales proporcionaran información y pruebas a los Estados Miembros y les prestaran asistencia en la investigación de los delitos cometidos dentro de las redes de las empresas;

f) Debería alentarse a las Naciones Unidas a investigar los motivos tras la aparente renuencia de los Estados a ratificar los tratados regionales relativos a las tecnologías de la información y las comunicaciones y a la ciberseguridad;

g) Debería adoptarse un criterio para un marco más sencillo de asistencia judicial recíproca, que tendría que ser aprobado por los Estados Miembros;

h) Por último, era necesario contar con un tratado internacional para hacer frente a las cuestiones de la delincuencia en la red tecnológica y digital. Un tratado de esa índole debería armonizar y proporcionar una orientación sucinta con respecto a la legislación, los principios de intercambio de información, las normas mínimas de seguridad de la información y las cuestiones de asistencia en la aplicación de la ley (investigación, extradición y enjuiciamiento) universales.

Brasil

52. El Brasil informó de que, desde la llegada de Internet, sus autoridades habían venido lidiando con los delitos cibernéticos y que esos delitos estaban aumentando en número y complejidad. La migración de distintos delitos a plataformas digitales había exigido un gran esfuerzo para actualizar las debidas respuestas legislativas y judiciales ante las nuevas amenazas. La amplitud geográfica de esos delitos había desafiado también los mecanismos tradicionales mediante los cuales el Brasil brindaba y recibía cooperación jurídica internacional. Los desafíos eran enormes: los proveedores de servicios de Internet, que poseían la información necesaria para investigar la ciberdelincuencia y reunir pruebas electrónicas, a menudo tenían su sede física en un país, prestaban servicios en distintos continentes y almacenaban su información en servidores localizados en cualquier otra parte del planeta. En ese contexto, los agentes de las fuerzas del orden se esforzaban por determinar quién tenía competencia sobre los datos y acceso directo a ellos y dirigirse debidamente a esa persona. Las solicitudes de cooperación internacional, a menudo canalizadas a través de tratados de asistencia judicial recíproca, se tramitaban muy lentamente y a veces quedaban privadas de efecto, dado el ritmo al que se eliminaban los datos digitales.

53. El Brasil también informó de que, cada vez que había un elemento internacional en las investigaciones y en la jurisdicción, el desarrollo jurídico de un caso solía ralentizarse debido a las divergencias con respecto al significado de la protección de la privacidad, conforme quedaba reflejado en los diversos requisitos nacionales en materia de divulgación de datos. Otra dificultad para la cooperación jurídica internacional era la extrema volatilidad de las pruebas digitales, puesto que la enorme cantidad de información que circulaba por todo el mundo y los costos de almacenamiento hacían que las empresas no conservaran los datos durante más tiempo del estrictamente necesario para sus negocios.

54. Entre los numerosos delitos que los agentes de las fuerzas del orden del Brasil habían perseguido en los medios digitales, la pornografía infantil era uno de los más frecuentes. El Brasil estaba sumamente comprometido a combatirla, bien por conducto de INTERPOL, bien de manera directa (se habían recibido 2 millones de informes de los Estados Unidos, por ejemplo). La invasión de sitios web y el *phishing* eran también delitos recurrentes. Ambos permitían el fraude bancario, que el sector financiero del Brasil había combatido mediante una respuesta proactiva y estructurada. El robo de bitcoines y la extracción de criptomonedas con fines maliciosos (por ejemplo, mediante el virus WannaCry en 2017) eran las tendencias más recientes y planteaban, además, dificultades para categorizar los delitos.

55. El Brasil era consciente de la peculiar naturaleza de las pruebas digitales y la ciberdelincuencia. En el artículo 11 de su Marco Civil de Internet, se disponía que cuando una de las terminales informáticas se encontrara en el territorio del Brasil habría de aplicarse el derecho brasileño a la recopilación, el almacenamiento y el tratamiento de los datos. Las empresas extranjeras que tuvieran sucursales en el Brasil o que prestaran servicios a usuarios brasileños y reunieran, almacenaran, mantuvieran o procesaran datos obtenidos de esos usuarios debían cumplir, por lo tanto, el derecho brasileño. Este Marco permitía que las autoridades tuvieran acceso directo a las pruebas electrónicas y a los datos recopilados a partir de los servicios prestados en el país. La jurisdicción del Brasil se basaba en el concepto de servicio ofrecido o proporcionado en su territorio nacional.

56. El Brasil opinó que, si bien Internet era un espacio virtual sin fronteras, su punto de conexión con el mundo físico se producía en el territorio existente y delimitado de un Estado. Una distribución internacional cohesionada de la jurisdicción representaría un paso adelante en la persecución de los delitos cibernéticos. En 2014 se incorporó al derecho brasileño una prueba para determinar si los imputados habían elegido una jurisdicción ventajosa (similar a la iniciativa de la Unión Europea en materia de pruebas electrónicas[7]). Incluso antes de que se negociara un tratado mundial al respecto, el Brasil había previsto la futura armonización de las legislaciones nacionales utilizando el mecanismo jurídico de la prueba ya mencionada, que no tenía en cuenta la ubicación de los servidores ni la nacionalidad de la empresa custodia.

57. El Brasil afirmó que se necesitaba una mayor y mejor cooperación, ya fuera a través de una modalidad avanzada de aplicación de los tratados de asistencia judicial recíproca vigentes o mediante tratados complementarios sobre ciberdelincuencia, que serían fundamentales para acelerar el intercambio internacional de las pruebas digitales, intrínsecamente efímeras. La multitud de plataformas, sistemas y estrategias que caracteriza a la ciberdelincuencia también exige una mayor cooperación técnica. Los expertos, agentes de policía, fiscales y jueces pertinentes deberían tener más oportunidades para aprender de las experiencias y los métodos con los que sus homólogos extranjeros habían obtenido buenos resultados.

58. El Brasil afirmó asimismo que la negociación multilateral de un instrumento internacional bajo los auspicios de las Naciones Unidas podría ser una forma de establecer unas normas mínimas comunes para el intercambio de información y pruebas a fin de hacer frente a la ciberdelincuencia, aprovechando los instrumentos internacionales y regionales ya existentes. Esas deliberaciones deberían organizarse con el apoyo de la UNODC, en Viena, donde ya se contaba con conocimientos especializados en la lucha contra el delito cibernético y donde el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético ya estaba examinando la cuestión. Un primer paso en la creación de una convención sobre la ciberdelincuencia podría ser convocar a un grupo de expertos de composición abierta que empezara a redactar un texto.

Canadá

59. El Canadá informó de que, si bien sus leyes se habían actualizado recientemente para combatir mejor la delincuencia en el siglo XXI, seguían existiendo algunos retos. Puso de relieve dos formas en que la comunidad internacional ya había venido trabajando para hacer frente a las condiciones subyacentes de esos retos.

60. En primer lugar, desde el punto de vista del proceso, el Canadá destacó la importante labor del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético. El Grupo tenía por cometido realizar un estudio exhaustivo del problema del delito cibernético y las respuestas frente a él, con miras a

[7] Decisión marco 2008/978/JAI del Consejo de la Unión Europea de 18 de diciembre de 2008 relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal (*Diario Oficial de la Unión Europea*, L 350, 30 de diciembre de 2008).

examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional y proponer respuestas nuevas. Esta labor estaba en curso y se regía por un plan de trabajo conforme al cual el Grupo finalizaría su labor en 2021. El Canadá consideró que la labor del Grupo, que brindaba un foro para que los expertos participaran en las deliberaciones acerca del tema sumamente técnico de la ciberdelincuencia, incluidas sus dimensiones de cooperación internacional y fomento de la capacidad, era esencial para las futuras deliberaciones en el seno de las Naciones Unidas respecto de posibles respuestas a la ciberdelincuencia.

61. En segundo lugar, desde un punto de vista sustantivo, el Canadá apoyaba plenamente el Convenio sobre la Ciberdelincuencia del Consejo de Europa por considerarlo el mejor instrumento internacional para combatir la ciberdelincuencia. El Convenio trataba eficazmente la naturaleza global del uso indebido y delictivo de las tecnologías de la información y las comunicaciones, mediante la prestación de cooperación internacional en la lucha contra la ciberdelincuencia, a través de las 63 partes con las que ya contaba, entre ellas un número considerable y creciente de Estados no europeos. El Convenio podía adaptarse a los nuevos desafíos mediante la publicación de notas de orientación que ayudaran a las partes a aplicar las disposiciones existentes a los nuevos fenómenos dentro de la ciberdelincuencia, complementadas por la Red 24/7 y sólidos programas de creación de capacidad. Las partes en el Convenio también estaban tratando de mejorar los mecanismos de cooperación internacional, pues las investigaciones penales requerían cada vez más el acceso a información almacenada en otras jurisdicciones. El Canadá apoyaba el Convenio y creía firmemente que era la mejor opción disponible, ya fuera como marco jurídicamente vinculante para los países que quisieran y pudieran adherirse a él, o como modelo para la elaboración de legislación nacional en los países que no se adhirieran.

62. Respecto a los problemas creados por los nuevos avances tecnológicos, el Canadá recordó que las comunicaciones eran ubicuas: en cualquier lugar y momento, por parte de cualquier proveedor o en cualquier dispositivo. Esto afectaba a la tarea de hacer cumplir la ley. A menudo, los investigadores debían tener en cuenta la naturaleza de los acuerdos de asociación, la propiedad de los bienes y la ubicación de las entidades en un entorno globalizado. Lo que parecía ser un único servicio para el usuario final estaba casi siempre integrado por múltiples servicios, múltiples tecnologías y múltiples formas de propiedad y distribución por múltiples jurisdicciones.

63. Por otra parte, el Canadá declaró que las conductas delictivas relacionadas con las tecnologías de la información y las comunicaciones seguían cambiando y adaptándose. Cada vez su ánimo de lucro era mayor, estaban adoptando un carácter transnacional y a menudo eran organizadas y especializadas. La labor delictiva se dividía en una serie de actividades menores, a menudo realizadas por distintos delincuentes, de los cuales cada uno desempeñaba una función dentro de la empresa delictiva. Esta especialización no solo aumentaba el nivel de complejidad, sino que también podía brindar mayor protección, puesto que algunos elementos constitutivos podrían no estar tipificados como delitos en algunas jurisdicciones. Además, los elementos del delito podrían estar dispersos por diversas jurisdicciones. Aprovechar las redes distribuidas de las cibertecnologías no solo explotaba las flaquezas de los sistemas de justicia nacionales, sino que también hacía que la territorialidad y la soberanía de los países se volvieran contra ellos.

64. El Canadá, centrándose en las dificultades de aplicar el derecho interno cuando su aplicabilidad estaba limitada territorialmente, informó de que las leyes se limitaban normalmente a un territorio determinado, y de ahí surgía un gran problema, puesto que las fronteras a menudo eran irrelevantes en un mundo cada vez más digital. Las tecnologías de la información y las comunicaciones seguían desarrollándose y evolucionando a un ritmo vertiginoso, al mismo tiempo que los delitos cibernéticos (como el uso indebido o la explotación de las tecnologías de la información y las comunicaciones) proliferaban y evolucionaban consecuentemente. La naturaleza efímera y transitoria de las pruebas digitales sumaba complejidad. Con tan solo pulsar una tecla, podían borrarse o trasladarse rápidamente de una jurisdicción a otra. Además, las importantes preocupaciones en materia de privacidad y derechos humanos y la

manera de ocuparse de ellas en un entorno digital entrañaban complicaciones. En las leyes tradicionales se conferían facultades de investigación que seguían siendo útiles en la lucha contra la ciberdelincuencia, pero también hacían falta instrumentos jurídicos nuevos o más complejos para velar por que la capacidad investigadora pudiera seguir el ritmo al que la tecnología se explotaba con fines delictivos.

65. El Canadá señaló que, desde un punto de vista práctico, uno de los desafíos vinculados a la obtención de la información necesaria a partir de otros Estados era saber dónde se encontraban los datos, si estaban disponibles y si su formato era comprensible. Hasta cierto punto, esto dependía de qué tipo de datos informáticos fueran. Algunos podían almacenarse con el fin de mantenerse disponibles a largo plazo, mientras que otros tipos de datos, como los de tráfico, podían ser más transitorios. El alcance de las empresas de telecomunicaciones era mundial, pero esas empresas solían estar supeditadas a las leyes nacionales o regionales: la manera de acceder a los datos o de conservarlos podía variar de un país a otro. Preocupaban al Canadá algunos regímenes de conservación de datos, dadas las considerables repercusiones en materia de privacidad y su falta de apoyo público. Para el Canadá, los regímenes de conservación específicamente desarrollados para la investigación, conforme se presentaban en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, brindaban una alternativa prudente. Además, las negociaciones relativas al segundo protocolo adicional al Convenio reforzarían la cooperación internacional y el acceso a las pruebas en la nube.

66. En relación con los desafíos del actual marco de cooperación internacional, el Canadá consideró que la obtención de pruebas digitales, tanto nacional como internacionalmente, era primordial para que la investigación y el enjuiciamiento de los delitos cibernéticos y de otros tipos de delitos graves obtuvieran buenos resultados. Sin embargo, las consecuencias de cruzar fronteras unilateralmente para obtener pruebas digitales, por cruciales que estas pruebas fueran, podían tensar las relaciones internacionales y menoscabar la validez de la búsqueda.

67. El Canadá afirmó que los tratados de asistencia judicial recíproca se utilizaban principalmente para obtener esa información. También declaró, sin embargo, que los procesos actuales no siempre eran lo bastante oportunos para las exigencias de las investigaciones en las que había pruebas electrónicas, ni tampoco estaban diseñados para el elevado volumen de solicitudes motivadas por los tan numerosos y diversos delitos que dejaban tras de sí huellas en forma de pruebas digitales. Para el Canadá, los mecanismos de asistencia judicial recíproca dispuestos en el Convenio sobre la Ciberdelincuencia del Consejo de Europa eran, actualmente, el mejor medio para poner en práctica la cooperación internacional entre diversos Estados partes. Además, las negociaciones relativas al segundo protocolo adicional al Convenio reforzarían aún más la cooperación internacional y ofrecerían un acceso a las pruebas en la nube fundamentado en tratados.

China

68. China, acogiendo con beneplácito la aprobación por la Asamblea General de la resolución 73/187, titulada “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, observó que, en varias resoluciones sobre la prevención del delito y la justicia penal, la Asamblea General había recalcado el fortalecimiento de la cooperación internacional en la lucha contra la ciberdelincuencia. China recomendó que la Asamblea General deliberara acerca del tema de la ciberdelincuencia en cada uno de sus períodos de sesiones, y que estudiara también la posibilidad de autorizar el establecimiento de los mecanismos intergubernamentales especiales pertinentes. Al mismo tiempo, China manifestó su apoyo a que se siguiera deliberando sobre la ciberdelincuencia en el marco de la Comisión de Prevención del Delito y Justicia Penal. También apoyó la labor que desempeñaba el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético a fin de examinar a fondo las cuestiones sustantivas de la lucha contra la ciberdelincuencia, de conformidad con su plan de trabajo para el período 2018–2021, y de presentar recomendaciones y conclusiones a la Comisión de

Prevención del Delito y Justicia Penal. China alentó también a distintas organizaciones regionales o internacionales a que debatieran activamente las cuestiones relacionadas con la ciberdelincuencia y a que trabajaran conjuntamente en las respuestas.

69. Por lo que respectaba a la legislación internacional, China opinó que la Convención contra la Delincuencia Organizada no podía responder eficazmente a las nuevas exigencias en materia de cooperación internacional para hacer frente a los delitos cibernéticos. Ya existían algunos tratados regionales relativos a la lucha contra la ciberdelincuencia, como los formulados por el Consejo de Europa, la Organización de Cooperación de Shanghái, la Liga de los Estados Árabes y la Unión Africana. Dadas las diferencias por lo que respecta al alcance de Estados miembros y al contenido de esos tratados, la legislación internacional contra la ciberdelincuencia era fragmentaria. Por eso, China afirmó que la comunidad internacional necesitaba establecer urgentemente un marco jurídico mundial contra el delito cibernético y trabajar de manera conjunta para hacer frente a la situación de la delincuencia, cada vez más grave, especialmente a los desafíos planteados por las nuevas tecnologías, como la computación en la nube, la inteligencia artificial, la Internet de las cosas y las criptomonedas. China coincidía con la opinión de que todos los Estados deberían negociar y establecer una convención mundial contra el delito cibernético abierta a todos los países, bajo los auspicios de las Naciones Unidas y sobre la base de la experiencia de los tratados regionales existentes.

70. Según China, la convención mundial sobre el delito cibernético debería coordinar eficazmente las leyes y prácticas nacionales contra la ciberdelincuencia, responder de manera oportuna a los nuevos problemas planteados por el desarrollo tecnológico y brindar soluciones aceptadas universalmente para la gobernanza mundial del delito cibernético. En lo que respecta al ámbito de aplicación, la convención debería aplicarse, además de a los delitos contra los sistemas informáticos, a los delitos cometidos principalmente mediante el uso de Internet y la tecnología de la información, así como a las actividades para facilitar y preparar la comisión de esos delitos. Por lo que a la aplicación de la ley y la investigación se refería, se deberían establecer en la convención medidas específicas de aplicación de la ley e investigación, e incluir disposiciones sobre cuestiones relacionadas con las alianzas público-privadas, en las que se aclararan las obligaciones de los proveedores y operadores de servicios de la red de cooperar en la prevención del delito cibernético y en la prestación de asistencia para la aplicación de la ley y la investigación. Con respecto a la cooperación internacional, la convención debería regular la práctica del diligenciamiento transfronterizo de pruebas electrónicas, diseñar un mecanismo más eficiente para el diligenciamiento de pruebas, basado en el respeto de la soberanía de los Estados y salvaguardando los derechos corporativos e individuales, y establecer disposiciones para el sistema jurisdiccional que fueran compatibles con las características de la ciberdelincuencia. Asimismo, en la convención deberían figurar disposiciones sobre mecanismos de creación de capacidad, asistencia técnica y prevención del delito.

71. En cuanto a la cooperación internacional, China señaló que, antes de introducir una convención mundial, se alentaba a los países a colaborar pragmáticamente contra el delito cibernético, sobre la base de la igualdad y el respeto y beneficio mutuos, de conformidad con la Convención contra la Delincuencia Organizada, los convenios y convenciones regionales y los tratados bilaterales. China también observó que algunos países habían promulgado legislación interna para eludir los cauces de la asistencia judicial y la cooperación en la aplicación de la ley y habían llevado unilateralmente datos electrónicos al extranjero, lo que, a su vez, había vulnerado los principios básicos del derecho internacional, como la soberanía y la protección de los derechos individuales y corporativos. China continuaba buscando un equilibrio entre el respeto de la soberanía nacional, la protección de los derechos individuales y corporativos y la facilitación de las investigaciones, y seguía mejorando la eficiencia de la obtención de pruebas mediante la optimización de los procedimientos de asistencia judicial y cooperación en materia de aplicación de la ley y mediante la innovación de los modelos de cooperación.

72. Con respecto a las medidas internas, China sostuvo que los Estados deberían adoptar las medidas correspondientes a nivel nacional para luchar eficazmente contra la ciberdelincuencia, en particular:

a) Penalizar el uso de Internet con fines terroristas y las actividades que facilitaran y prepararan la comisión de delitos cibernéticos;

b) Determinar las obligaciones que tenían los proveedores y operadores de servicios de Internet de cooperar en la prevención de la ciberdelincuencia y la prestación de asistencia en materia de aplicación de la ley e investigación y, al mismo tiempo, aclarar los límites de esas obligaciones y garantizar los derechos de las empresas y los particulares pertinentes;

c) Mejorar la capacidad necesaria de los órganos encargados de hacer cumplir la ley y los órganos judiciales para investigar los delitos cibernéticos, especialmente para afrontar mejor las dificultades planteadas por las nuevas tecnologías;

d) Reconocer el efecto probatorio de los datos electrónicos y fijar una definición de las pruebas electrónicas y su alcance;

e) Aclarar las normas para la obtención y admisión de pruebas electrónicas y disponer en el derecho interno medios como la incautación y el cierre de los medios de almacenamiento originales, la recopilación *in situ*, la inspección remota y el embargo preventivo;

f) Tener en cuenta la especificidad de las pruebas electrónicas al aplicar las normas tradicionales que regían la práctica de la prueba;

g) Reforzar el fomento de la capacidad de los encargados de obtener pruebas electrónicas, dotar a los equipos profesionales de conocimientos básicos de derecho y capacidad técnica, y formular normas técnicas sobre la obtención de pruebas electrónicas.

Colombia

73. El Gobierno de Colombia coincidió en la necesidad de mejorar la coordinación y la cooperación entre los Estados en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, a través de asistencia técnica a los países en desarrollo para mejorar a su legislación nacional y reforzar la capacidad de sus autoridades nacionales de prevenir, detectar, investigar y enjuiciar dichas actividades delictivas. Sin embargo, consideró importante diferenciar entre los temas relativos a la ciberdelincuencia y una posible regulación amplia sobre las tecnologías de la información y las comunicaciones, que iría más allá de la regulación penal sobre los actos ilícitos. Por consiguiente, es muy importante tener claros los conceptos sobre la regulación del uso de las tecnologías de la información y las comunicaciones con fines delictivos, con la seguridad de la información y las telecomunicaciones en el contexto de la seguridad internacional. Colombia estaba a favor de un Internet libre, abierto y seguro, y consideró fundamental que los países contaran con las herramientas que les permitieran cooperar en la lucha contra la ciberdelincuencia; que fortalecieran sus capacidades nacionales, y que se consolidaran las medidas de confianza entre los países.

74. Colombia afirmó que había grandes desafíos en materia de ciberdelincuencia, por ejemplo, la identidad digital; la cooperación con proveedores de servicios de Internet; asuntos relacionados con las pruebas digitales, técnicas para su obtención, almacenamiento, cadena de custodia, certificación y validez; la protección de datos, la intimidad y el respeto de los derechos y libertades de las personas. Además, el delito cibernético estaba estrechamente relacionado con otros delitos que trascendían fronteras. Por eso, Colombia opinó que se requería una comprensión más profunda de los delitos, de sus *modus operandi*, etc., y por ello era importante que se compartieran las experiencias y buenas prácticas entre los países para mejorar las respuestas nacionales e internacionales para contrarrestarlos. La brecha digital hace que algunos

países sean más vulnerables y la cooperación no sea efectiva. La cooperación judicial internacional (como la asistencia judicial recíproca, las solicitudes de asistencia judicial recíproca y los tratados de asistencia judicial recíproca) debe adaptarse para que funcione con mayor celeridad. Para tal efecto, Colombia propuso diseñar protocolos y formatos que facilitaran el entendimiento de los países y fueran válidos en el marco de los procesos de investigación y judicialización.

75. Sin embargo, Colombia consideró también que los temas referidos al delito cibernético debían seguir siendo discutidos, desde el punto de vista técnico y político, por la Comisión de Prevención del Delito y Justicia Penal a través del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético. Este debería constituir el foro principal, y no deberían generarse nuevos grupos alternos que limitaran la participación de los países. El Grupo de Expertos ha acordado un plan de trabajo, que espera culminar en 2021 con un informe que presente las opciones para fortalecer las respuestas actuales y proponer nuevas respuestas jurídicas o de otra índole.

76. Finalmente, Colombia consideró que no era necesario comenzar la negociación de un nuevo convenio sobre ciberdelincuencia partiendo de cero. Para Colombia era fundamental dar prioridad a la creación de capacidades y la cooperación sobre la base de los tratados existentes, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Costa Rica

77. Costa Rica indicó que, debido a su amplia trayectoria en el reconocimiento, respeto y defensa de los derechos humanos, los instrumentos internacionales que había suscrito y ratificado no violaban la soberanía del Estado costarricense.

78. Costa Rica opinó que los fiscales e investigadores de las causas relacionadas con ciberdelincuencia debían lograr un equilibrio, al atender a una víctima, entre el derecho a la privacidad de las personas y la seguridad pública; esas garantías debían respetarse al recopilar los elementos de prueba, para lo cual se debía solicitar a un juez las respectivas solicitudes de allanamiento, de levantamiento de secreto bancario o de levantamiento de secreto tributario, entre otras. Todo ello resultaba necesario para lograr éxito en las investigaciones, así como para garantizar la admisibilidad de las pruebas ante el tribunal.

79. Costa Rica, al ser Estado Parte en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, había tenido acceso a una amplia capacitación para los profesionales del derecho, así como a la Red 24/7 y a intercambios con otros funcionarios de otras latitudes, a efectos de obtener e intercambiar información pertinente para investigar en tiempo real las causas y obtener la prueba digital. Adicionalmente, al ser Costa Rica un Estado parte en el Convenio sobre la Ciberdelincuencia, ha sido incorporada al proyecto del Consejo de Europa y la Unión Europea denominado Acción Global contra la Ciberdelincuencia (GLACY+), con lo cual ha participado en las siguientes actividades:

a) Misión de evaluación inicial del Proyecto GLACY+, realizada en San José del 21 al 24 de mayo de 2018;

b) Misión consultiva sobre legislación relativa a delitos cibernéticos y pruebas electrónicas y misión consultiva sobre política y estrategia nacionales en materia de ciberdelincuencia. Elaboración y revisión del marco legislativo sobre ciberdelincuencia y pruebas digitales y elaboración y revisión de la política nacional en materia de ciberdelincuencia, que tuvieron lugar en San José del 8 al 11 de octubre de 2018;

c) Formación judicial de capacitadores sobre ciberdelincuencia y pruebas electrónicas para jueces, fiscales y abogados, impartida en San José del 11 al 15 de febrero de 2019;

d) Curso avanzado de capacitación judicial en delitos cibernéticos y pruebas electrónicas para jueces, fiscales y otros funcionarios judiciales (del 13 al 16 de mayo

de 2019), y misión consultiva sobre legislación procesal relativa a delitos cibernéticos y pruebas electrónicas (los días 16 y 17 de mayo de 2019).

80. Adicionalmente, el Proyecto GLACY+ ha apoyado la participación de Costa Rica en las siguientes actividades en el extranjero:

a) Taller internacional sobre estrategias de capacitación judicial en materia de delito cibernético y pruebas electrónicas, realizado en Cebu (Filipinas) del 12 al 14 de diciembre de 2017;

b) Conferencia internacional conjunta del Consejo de Europa y Eurojust sobre la cooperación judicial en materia de ciberdelincuencia, celebrada en La Haya (Países Bajos) los días 7 y 8 de marzo de 2018;

c) Cuarta Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, celebrada en Viena del 3 al 5 de abril de 2018;

d) 27º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal y reunión del Comité de Dirección de la Acción Global contra la Ciberdelincuencia (GLACY+), celebrados en Viena del 14 al 18 de mayo de 2018;

e) Reunión del Comité del Convenio sobre la Ciberdelincuencia (T-CY), 19ª Reunión Plenaria del T-CY, Segunda Reunión Plenaria para la Redacción del Protocolo, Conferencia Octopus de Cooperación contra la Ciberdelincuencia y Seminario sobre la Red 24/7, celebrados en Estrasburgo (Francia) del 9 al 13 de julio de 2018;

f) Taller internacional conjunto para dependencias de investigación de delitos cibernéticos y autoridades centrales, celebrado en Singapur del 27 al 31 de agosto de 2018;

g) Cuarta Reunión del Grupo de Trabajo sobre Ciberdelincuencia para Jefes de las Dependencias, celebrada en Río de Janeiro (Brasil) del 4 al 6 de septiembre de 2018;

h) Conferencia sobre Economía Sumergida y Ciberdelincuencia, celebrada en Estrasburgo (Francia) del 4 al 7 de septiembre de 2018;

i) Sexta Conferencia de INTERPOL y Europol sobre Ciberdelincuencia, celebrada en Singapur del 18 al 20 de septiembre de 2018;

j) 20ª Reunión Plenaria del T-CY, Tercera Reunión Plenaria para la Redacción del Protocolo, Reunión del Comité de GLACY+, celebradas en Estrasburgo (Francia) del 27 al 30 de noviembre de 2018;

k) Conferencia sobre Justicia Penal en el Ciberespacio, celebrada en Bucarest del 25 al 27 de febrero de 2019;

l) Curso de desarrollo de instructor de INTERPOL, impartido en Bogotá del 25 de febrero al 1 de marzo de 2019;

m) Quinta Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, celebrada en Viena del 27 al 29 de marzo de 2019.

81. Actualmente, el Convenio sobre la Ciberdelincuencia del Consejo de Europa ha sido ratificado por 63 países del mundo (tanto del continente europeo como de otras latitudes), por lo que, para Costa Rica, es un instrumento internacional que posee trayectoria en su implementación.

Chequia

82. Chequia comunicó que había ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa en 2013. En 2014 procedió a ratificar el Protocolo Adicional al Convenio, que prestaba especial atención a la penalización de los actos racistas y xenófobos cometidos por medio de sistemas informáticos, y con el que se ampliaba el alcance del Convenio y sus disposiciones sustantivas, procesales y en materia de

cooperación internacional. El Convenio y su Protocolo Adicional están abiertos a todos los países, no solo a los Estados miembros del Consejo de Europa.

83. Chequia creía firmemente que el Convenio sobre la Ciberdelincuencia del Consejo de Europa era el instrumento más eficiente y actualizado para hacer frente a todos los desafíos derivados del fenómeno de la ciberdelincuencia en todo el mundo. Por eso celebraba el número cada vez mayor de Estados no miembros del Consejo de Europa que recientemente se habían adherido al Convenio o habían estudiado la posibilidad de hacerlo, lo que ponía de relieve la naturaleza interregional de este y la inclusividad y transparencia de sus procedimientos de adhesión. Por consiguiente, en lugar de elaborar un nuevo instrumento, que sería más bien contraproducente dado el largo proceso que entrañaba aprobar y ratificar las convenciones de las Naciones Unidas, la atención debería centrarse en la aplicación efectiva de los instrumentos jurídicos existentes representados por el Convenio sobre la Ciberdelincuencia del Consejo de Europa, teniendo en cuenta también la contribución positiva de este a la armonización de las normas legislativas nacionales.

84. Chequia apoyaba y elogiaba los conocimientos técnicos especializados garantizados por la UNODC y sus resultados concretos, como la Guía Práctica para la Solicitud de Pruebas Electrónicas Transfronterizas. Debería seguir centrándose la atención en los aspectos expertos de la cuestión, previstos en las deliberaciones del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, con sede en Viena, que aporta un singular valor a nivel de las Naciones Unidas.

85. Chequia afirmó que reforzar las normas procesales con miras a combatir los delitos cibernéticos era de vital importancia; los derechos humanos y las salvaguardias del estado de derecho, incluida la protección de datos personales, eran igualmente importantes.

86. Consciente del creciente número de amenazas relacionadas con la ciberdelincuencia y su carácter cada vez más transfronterizo, Chequia comunicó que se estaba centrando en concienciar y capacitar con respecto a la ciberamenaza, por ejemplo, con el fomento de la capacidad y la contratación de nuevo personal encargado de hacer cumplir la ley con los conocimientos especializados necesarios. En ese contexto, la Red Nacional de Fiscales, que funcionaba a nivel regional y estaba especializada en la esfera de la ciberdelincuencia, y el establecimiento de dependencias policiales especializadas en ciberdelincuencia se había percibido como iniciativas muy positivas desde el punto de vista de la lucha contra el delito cibernético. Además, se informó de que se estaba haciendo hincapié en las pruebas electrónicas, cuyo volumen se había incrementado notablemente en las actuaciones penales. Con vigencia a partir del 1 de febrero de 2019, Chequia había aprobado una nueva reglamentación jurídica en la que se sentaban normas explícitas para la conservación rápida de los datos informáticos almacenados, tanto en los casos nacionales como en los transnacionales.

87. La digitalización de la justicia era una de las prioridades del Ministerio de Justicia de Chequia. El Gobierno había aprobado la Estrategia Conceptual Nacional de Lucha contra la Ciberdelincuencia (esta cuestión queda reflejada en la Estrategia Conceptual Nacional de Lucha contra la Delincuencia Organizada, actualizada periódicamente y publicada por el Ministerio del Interior), en la que se habían fijado metas y medidas definidas que habría que adoptar en esa esfera.

88. Por lo que respectaba a la asistencia judicial recíproca, Chequia informó de que las solicitudes de asistencia y las operaciones conexas se tramitaban, cada vez en mayor medida, de manera electrónica. Se habían simplificado los procedimientos pertinentes a fin de lograr una mayor eficiencia y una pronta cooperación, en particular en el intercambio de información entre los Estados (por ejemplo, mediante el establecimiento de canales de comunicación oficiosos o puntos de contacto dentro de la Red 24/7 con arreglo al Convenio sobre la Ciberdelincuencia del Consejo de Europa).

89. Chequia mencionó los mismos posibles desafíos que otros países: el creciente anonimato de los usuarios (el cifrado como norma), la disponibilidad de programas maliciosos y servicios ilícitos de pago (el delito como servicio) y las posibilidades de

ocultar los beneficios obtenidos del delito en monedas virtuales, así como el anonimato que de ello se desprendía. Por último, pero no por ello menos importante, Chequia destacó que el mencionado sistema de asistencia judicial recíproca internacional no era suficiente para las cuestiones cibernéticas, en particular dada su lentitud. El plazo medio de tramitación de una solicitud de asistencia judicial recíproca relativa a cuestiones cibernéticas era de 21 meses (entre los Estados miembros del Consejo de Europa). Por lo tanto, convenía comenzar a debatir la definición de jurisdicción en el ciberespacio y el acceso directo a las pruebas electrónicas ubicadas en servidores situados en el extranjero (o en paradero desconocido). Había margen para deliberar acerca de la cooperación directa con los proveedores extranjeros de servicios. Chequia, como Estado miembro de la Unión Europea y del Consejo de Europa, había venido participando en numerosos debates al respecto, sobre todo en relación con las órdenes europeas de producción y conservación y el segundo protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa.

República Popular Democrática de Corea

90. El Gobierno de la República Popular Democrática de Corea era del parecer de que las tecnologías de la información y las comunicaciones no deberían utilizarse en actividades delictivas de manera que amenazaran o quebrantaran la estabilidad política, económica y social de los Estados. Consideraba que, a fin de evitar que las tecnologías de la información y las comunicaciones se utilizaran con fines delictivos, la cooperación y coordinación entre Estados eran sumamente importantes.

91. Teniendo presente la insuficiencia mundial de instrumentos jurídicos para prevenir y combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, la República Popular Democrática de Corea opinó que sería necesario preparar una resolución de las Naciones Unidas en materia de cooperación para evitar la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, en consonancia con los intereses de los Estados.

92. El Gobierno de la República Popular Democrática de Corea destacó que la cuestión de la utilización de las tecnologías de la información y las comunicaciones en las actividades delictivas debería debatirse en la reunión del grupo de expertos de composición abierta pertinente y con la participación de todos los Estados interesados.

El Salvador

93. El Gobierno de El Salvador consideró que la ausencia de legislación era el principal desafío en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y, en ese sentido, indicó las siguientes consideraciones:

a) La ausencia de controles o legislación que regulara la asignación de telefonía móvil y uso de Internet, para todas las personas en general, con más énfasis en los teléfonos prepago, que fácilmente se podían adquirir y utilizar para cualquier fin;

b) La ausencia de legislación para poder obtener información en línea y en tiempo real sobre bitácoras de uso y asignaciones de direcciones IP públicas y privadas de los diferentes operadores que se encontraban en el país;

c) La ausencia de una regulación para el uso de dispositivos tecnológicos, como drones, bloqueadores de señal, interceptores, cualquier equipo infectado por un virus y otros equipos, que permitan cometer actos de ciberdelincuencia;

d) La ausencia de una regulación que obligara a los administradores de red de instituciones públicas, privadas o sin fines de lucro a establecer, mantener y resguardar las bitácoras de conexión de sus clientes internos. La falta de esa regulación se utilizaba y podía utilizarse para cometer delitos tradicionales y cibernéticos.

Estonia

94. Estonia afirmó que la ciberdelincuencia y la utilización de las tecnologías de la información y las comunicaciones con fines delictivos eran fenómenos crecientes y planteaban desafíos a las entidades encargadas de hacer cumplir la ley de todo el mundo.

95. Estonia señaló que, dado que la mayoría de los delitos cibernéticos eran de naturaleza transfronteriza, la cooperación internacional revestía máxima importancia. Era frecuente que las pruebas electrónicas relacionadas con un delito se almacenaran fuera del país encargado de la investigación criminal. Sin embargo, la cooperación internacional no siempre era eficaz y a menudo los países carecían del derecho sustantivo y procesal necesarios o de la suficiente capacidad entre las entidades encargadas de hacer cumplir la ley y el poder judicial.

96. Estonia afirmó que, en la actualidad, el único instrumento jurídicamente vinculante para luchar contra la ciberdelincuencia que tenía repercusión mundial era el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Muchos países del mundo que no se habían adherido al Convenio habían utilizado como ejemplo sus disposiciones en materia de derecho sustantivo y procesal y de cooperación internacional. Dado que esas normas habían sido aceptadas por muchos países y que ya había cierto nivel de armonización, era necesaria y posible una mayor cooperación. El Convenio, como instrumento internacional jurídicamente vinculante ya vigente, brindaba normas que deberían por lo tanto cumplirse también en los países donde no se contara con el marco jurídico necesario.

97. Según Estonia, el Convenio sobre la Ciberdelincuencia del Consejo de Europa había sido un instrumento eficaz para la recopilación y el intercambio de pruebas electrónicas. Como las disposiciones y medidas de derecho procesal del Convenio también se podían utilizar para otros delitos relacionados con datos informáticos o pruebas electrónicas, dicho Convenio era más que un mero instrumento sobre ciberdelincuencia. Además, puesto que sus disposiciones se podían aplicar a las pruebas electrónicas relacionadas con cualquier delito, el Convenio se había vuelto aún más útil y valioso para los Estados. Las pruebas electrónicas y el acceso a ellas eran uno de los mayores retos para las autoridades encargadas de hacer cumplir la ley al realizar investigaciones criminales. Dado que a menudo las pruebas electrónicas estaban almacenadas en otros países, había que utilizar medidas y canales de cooperación internacional. Si bien la cooperación internacional sobre la base del Convenio sobre la Ciberdelincuencia del Consejo de Europa y otros instrumentos (como la Convención contra la Delincuencia Organizada) funcionaba, era necesario mejorarla y hacerla más eficaz.

98. Estonia señaló que durante varios años se habían mantenido deliberaciones acerca de un segundo protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa. Las negociaciones habían comenzado recientemente. El protocolo adicional, que estaría abierto a los Estados partes en el Convenio, brindaría instrumentos complementarios para las autoridades encargadas de hacer cumplir la ley y el poder judicial a fin de mejorar la cooperación internacional y proporcionar normas y salvaguardias más claras. Estonia declaró, por lo tanto, que el Convenio y su importancia y cobertura mundiales crecerían en el futuro y más países podrían aprovecharse de ello.

99. Estonia puso de relieve las deliberaciones acerca de la lucha contra la ciberdelincuencia y la creación de capacidad en el seno de la UNODC. Desde 2011, el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético había venido examinando posibles respuestas a la ciberdelincuencia, incluida la forma de velar por una mejor aplicación de los instrumentos internacionales vigentes. El Grupo de Expertos se había convertido en una plataforma útil y eficaz para que los Estados deliberaran acerca de los problemas y desafíos relacionados con la ciberdelincuencia y el intercambio de mejores prácticas. Aunque hasta la fecha no había habido consenso sobre muchas cuestiones, se había expresado un firme apoyo al fomento de la capacidad. El Grupo de Expertos proseguía su labor de conformidad con

el plan de trabajo acordado, y estaba previsto que ofreciera conclusiones y recomendaciones a más tardar en 2021.

100. Estonia consideró que sería prematuro entablar deliberaciones paralelas y preparar informes paralelos a nivel de las Naciones Unidas. Dado que los recursos eran limitados, deberían utilizarse de la manera más eficiente; por ello, el Grupo de Expertos existente debería proseguir y finalizar su labor en el marco de su mandato y de su plan de trabajo. Sin embargo, como ya habían demostrado las deliberaciones en curso, habían surgido nuevos temas y subtemas en relación con la ciberdelincuencia, las investigaciones en línea y las pruebas electrónicas, lo que podría hacer que el Grupo de Expertos continuara después de 2021.

Francia

101. Francia informó de que, en el contexto del Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, había afirmado -junto con otros más de 60 Estados y varios cientos de organizaciones internacionales, representantes de la sociedad civil y el sector privado- su apoyo a un ciberespacio abierto, seguro, estable, accesible y pacífico en el que fuera aplicable el derecho internacional, incluidos los derechos humanos. Una de las condiciones necesarias para lograr ese objetivo era la lucha contra la utilización de los medios digitales con fines delictivos.

102. En ese sentido, Francia informó de que contaba con un sólido sistema nacional en el ámbito de la lucha contra la ciberdelincuencia, por lo que respectaba al derecho vigente y a las medidas de prevención y los recursos específicos para que investigadores y jueces combatieran eficazmente el fenómeno. El mecanismo emanaba en parte de la transposición de las disposiciones del Convenio sobre la Ciberdelincuencia del Consejo de Europa, que brindaba un marco jurídico internacional apropiado y flexible para hacer frente al fenómeno de la ciberdelincuencia mediante el fortalecimiento de los sistemas legislativos nacionales, pero también allanando el camino de la cooperación internacional. Esas disposiciones se sumaban a las previstas en relación con todas las formas de delincuencia organizada transnacional en la Convención contra la Delincuencia Organizada.

103. Pese a ese marco jurídico internacional adoptado y a un robusto sistema nacional, Francia todavía se enfrentaba a algunas dificultades en la lucha contra la ciberdelincuencia. Esas dificultades se abordaban en el marco de las reuniones del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético y eran las siguientes:

a) La falta de adaptación, en varios países, de las leyes nacionales y los medios especializados a la lucha contra la ciberdelincuencia, en particular, una falta de legislación nacional en algunos países (tanto derecho sustantivo como procesal) que estuviera adaptada a la cuestión del delito cibernético y una falta de capacitación y recursos adaptados para los investigadores y agentes de la cadena penal a fin de combatir eficazmente la ciberdelincuencia. Con objeto de ayudar a fortalecer los mecanismos en esa esfera, Francia participaba activamente en varios programas de fomento de la capacidad de carácter bilateral, pero también a nivel de la Unión Europea y el Consejo de Europa;

b) La falta de cooperación por parte del sector privado y algunas jurisdicciones extranjeras en relación con la transferencia de datos, e incluso en la conservación de las órdenes de embargo preventivo en las investigaciones y procedimientos judiciales. La cooperación de los proveedores de servicios seguía siendo parcial hasta el momento (con un promedio del 60 %, pero muy variable dependiendo de los asociados). Era esencial que estos últimos respondieran a las solicitudes enviadas por las autoridades competentes de los Estados en el contexto de las investigaciones y los procedimientos penales, sin que esta respuesta estuviera supeditada a la nacionalidad adscrita a la dirección IP. A fin de mejorar el acceso a las pruebas electrónicas, Francia participaba activamente en las negociaciones en el seno de la Unión Europea de dos propuestas legislativas presentadas por la Comisión Europea el 27 de abril de 2018,

a saber, un proyecto de reglamento por el que se fijaban las condiciones de acceso a las pruebas electrónicas y un proyecto de directiva por la que se exigía a los proveedores de servicios designar a un representante legal facultado para recibir y responder a los requerimientos judiciales. Francia también participaba en el grupo de trabajo encargado de redactar un protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa, que también se ocupaba de esta cuestión;

c) El permanente desafío de adaptarse a las nuevas tecnologías, en particular, a las criptomonedas, que solo estaban parcialmente reguladas, lo cual daba lugar a grandes riesgos de anonimización de los flujos financieros, la red oscura, el cifrado y la Internet de las cosas. Las deliberaciones acerca de cómo entender mejor esos fenómenos y los intercambios de mejores prácticas al respecto se desarrollaban dentro del marco del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético y, de manera más amplia, dentro de la UNODC; y Francia quiso subrayar el valor operacional de esas deliberaciones e intercambios.

Georgia

104. Georgia informó de que, desde 2008, había realizado reformas esenciales a sus leyes sustantivas y procesales y a sus instrumentos en materia de políticas para luchar eficazmente contra el delito cibernético. Las principales reformas se habían armonizado con el Convenio sobre la Ciberdelincuencia del Consejo de Europa, al que Georgia se había adherido en 2012.

105. Georgia consideró que las dificultades de acceso a los datos transfronterizos eran uno de los principales retos en la lucha contra la ciberdelincuencia. Los mecanismos tradicionales de asistencia judicial recíproca se habían quedado en gran medida obsoletos dada la constante evolución de la computación en la nube. Georgia opinó que la desregulación o facilitación del acceso a los datos transfronterizos sería una reforma inevitable para incrementar la eficacia de la investigación y persecución de la ciberdelincuencia. Sin embargo, esas reformas las debían realizar los Estados a través de instrumentos multilaterales, y las facultades procesales interjurisdiccionales debían ir acompañadas de firmes salvaguardias. Georgia consideró que la redacción del segundo protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa brindaba una importante oportunidad en ese sentido.

106. Georgia informó de que, en los últimos años, había participado en varios proyectos de creación de capacidad ejecutados o apoyados por el Consejo de Europa (proyectos de la Asociación Oriental), la Unión Europea y el Gobierno de los Estados Unidos. Como parte de esos proyectos, varios cientos de profesionales de las fuerzas del orden y del poder judicial habían recibido capacitación y el Gobierno había aprobado varios documentos de políticas fundamentados en conocimientos multinacionales especializados en ciberdelincuencia, pruebas electrónicas y ciberseguridad.

107. Por lo que respectaba al derecho sustantivo, Georgia comunicó que el acceso y la interceptación ilícitos, la interferencia de datos y sistemas y el uso indebido de dispositivos se habían tipificado como delitos con arreglo a los artículos 284 a 286 del Código Penal de 1999, en consonancia con los artículos 2 a 6 del Convenio sobre la Ciberdelincuencia del Consejo de Europa. Todos los delitos relacionados con la cibernética se habían perseguido como delitos convencionales sin dificultades considerables. Por ejemplo, el ciberfraude era un delito que había ido en aumento recientemente, y los tribunales de Georgia no habían encontrado impedimento alguno para aplicar a esos casos la legislación tradicional en materia de fraude.

108. En relación con el derecho procesal, Georgia informó de que, desde 2010, había venido introduciendo en su legislación todas las facultades procesales previstas en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, entre ellas las órdenes de presentación, la obtención en tiempo real de datos de tráfico y la interceptación de contenido, si bien varias otras competencias ya estaban presentes en su legislación. Entretanto, Georgia había adoptado firmes garantías procesales, como la necesidad de una autorización judicial para todas las facultades procesales que supusieran una

intromisión de la intimidad, el requisito de la proporcionalidad, la limitación del uso de determinadas facultades procesales (que solo se utilizaban en caso de delitos graves) y el requisito de utilizar la opción menos intrusiva dentro de las facultades procesales de las que se dispusiera.

109. Con respecto a la cooperación de los proveedores de servicios de Internet extranjeros, se afirmó que los organismos encargados de hacer cumplir la ley de Georgia habían obtenido satisfactoriamente información sobre abonados de diversas empresas de Internet mundiales (Facebook, Apple, Microsoft, etc.), en conexión con los servicios prestados en Georgia. Por ejemplo, Georgia fue uno de los 10 países del mundo con mayor tasa de divulgación, que por parte de Facebook ascendía al 94 % respecto de solicitudes relacionadas con los procesos judiciales del período 2017–2018. En 2018, Georgia había introducido una orden de presentación internacional, que facultaba a los jueces de Georgia a emitir una orden de presentación respecto de personas o entidades ajenas a la jurisdicción territorial del país si concurrían los siguientes requisitos: consentimiento por parte de la persona sujeta a la orden para que los datos electrónicos se divulgaran, y permiso por parte del país anfitrión de la entidad extranjera para que se revelaran esos datos conforme a sus leyes o políticas ejecutivas. El fiscal debía obtener esas órdenes de un tribunal y por conducto de un funcionario autorizado por el Fiscal General. El incumplimiento de esas órdenes no entrañaba ninguna responsabilidad jurídica. Con arreglo al artículo 18 del Convenio sobre la Ciberdelincuencia del Consejo de Europa, Georgia se había servido de órdenes de presentación internacional con respecto a Facebook y otros proveedores de servicios internacionales en conexión con los servicios prestados en Georgia.

Alemania

110. Alemania hizo referencia a que el desarrollo tecnológico conducía a continuos cambios en la sociedad. Esos avances tecnológicos creaban nuevas oportunidades de las que tanto cada persona como el conjunto de la sociedad podían beneficiarse, pero también entrañaban nuevos desafíos. Las posibilidades que brindaba la tecnología para comunicarse y actuar con rapidez y en todo el mundo también se utilizaban con fines ilícitos. Por consiguiente, Alemania opinaba que era importante hacer frente a los desafíos y luchar contra las conductas delictivas. Para ello era necesario un marco jurídico nacional lo suficientemente desarrollado, pero también una cooperación eficaz que traspasara las fronteras nacionales.

111. Para Alemania, toda solución a nivel internacional debería adaptarse específicamente a los desafíos concretos planteados por las tecnologías de la información y las comunicaciones y debería referirse a las cuestiones de confidencialidad, integridad y acceso a los sistemas de información (los llamados delitos cibernéticos básicos). No sería ni factible ni conveniente tratar de contar con disposiciones aplicables a todos los delitos cometidos mediante la utilización de una computadora o por Internet. Las disposiciones sobre los delitos cibernéticos básicos han de ser lo suficientemente flexibles como para adaptarse a los avances tecnológicos. Por otra parte, se necesitaban mecanismos de intercambio transfronterizo de datos para investigar, enjuiciar y castigar los delitos cibernéticos.

112. Alemania destacó que el Convenio sobre la Ciberdelincuencia del Consejo de Europa era idóneo para hacer frente eficazmente a los desafíos existentes en la lucha contra la ciberdelincuencia. En ese sentido, el Convenio había demostrado ser un instrumento apropiado para combatir la ciberdelincuencia, abierto también a países terceros. Alemania observó que el Convenio era ampliamente aceptado por muchos Estados como principal instrumento internacional en la lucha contra el delito cibernético, y también las autoridades alemanas lo habían utilizado como guía para su derecho interno. La definición tecnológicamente neutra de los delitos que contenía el Convenio seguía estando al día. En opinión de Alemania, había sido precisamente esa atención, en general, a los delitos contra la confidencialidad, integridad y accesibilidad de los sistemas de información la que había contribuido a que el Convenio gozara de ese elevado nivel de aceptación mundial. Alemania consideraba importante, por lo tanto,

que se entendiera el concepto de un conjunto básico de delitos cibernéticos y que se mantuviera dicho concepto. En cambio, se debería proceder con cautela al ampliar el alcance de la “ciberdelincuencia” a conductas en las que los dispositivos informáticos se utilizaran únicamente como medio para cometer delitos generales. Casi todos los delitos podían cometerse utilizando dispositivos informáticos, pero eso no los convertía en “delitos cibernéticos”.

113. Alemania señaló que las adaptaciones a los acontecimientos más recientes deberían basarse en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, como sucedía actualmente con la negociación del segundo protocolo adicional, en la esfera de la obtención de pruebas electrónicas. El segundo protocolo adicional estaría destinado a mejorar la cooperación entre las partes respecto del rastreo de la ciberdelincuencia y la obtención de pruebas electrónicas. Por consiguiente, Alemania no secundaba los llamamientos a favor de la elaboración de un nuevo instrumento internacional sobre la ciberdelincuencia.

114. Además, el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético estaba realizando un amplio examen de los problemas en la lucha contra la ciberdelincuencia. Desde 2011 venían celebrándose deliberaciones sustantivas sobre los desafíos de la ciberdelincuencia en el seno del Grupo de Expertos. Según Alemania, el Grupo de Expertos era y debería seguir siendo el principal proceso a nivel de las Naciones Unidas relativo al tema de la ciberdelincuencia. En la medida de lo posible, convendría evitar procesos paralelos relacionados con las resoluciones de la Asamblea General y la posible duplicación de esfuerzos.

115. Alemania subrayó que se debería prestar especial atención a la aplicación de la legislación en materia de ciberdelincuencia y al logro de un progreso real sobre el terreno, entre otras cosas, mediante la prestación de asistencia técnica. No se carecía de normas internacionales adecuadas y, además, los Estados Miembros habían promulgado legislación sustantiva en materia de derecho penal para aplicar las normas vigentes. El desafío al que ahora debería hacer frente el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético era cómo brindar a las entidades encargadas de hacer cumplir la ley un marco jurídico sólido y los recursos necesarios para obtener pruebas electrónicas y, al mismo tiempo, delimitar las facultades de aplicación de la ley mediante condiciones y salvaguardias basadas en el estado de derecho y la protección de los derechos y libertades fundamentales.

Ghana

116. Ghana informó de que actualmente contaba con dos principales instrumentos legislativos en materia de pruebas cibernéticas electrónicas: la Ley de Comunicaciones Electrónicas de 2008 (Ley 775) y la Ley de Transacciones Electrónicas de 2008 (Ley 772).

117. En Ghana, aunque el Fiscal General era el principal fiscal de todos los delitos, otros organismos, como la policía, también podían iniciar acciones judiciales bajo la autoridad del Fiscal General. La Fiscalía General, sin embargo, enjuiciaba los casos que le remitía la policía. El número de casos de ciberdelincuencia y delitos facilitados por la informática que la policía remitía a la Fiscalía era menor y, por lo tanto, se habían observado unos pocos problemas y contratiempos en el enjuiciamiento de esos casos.

118. Ghana informó de que la policía, el principal órgano de investigación, carecía de los instrumentos necesarios, puesto que todos los instrumentos de los laboratorios forenses para la lucha contra la ciberdelincuencia habían expirado. Las investigaciones se encomendaban, por lo tanto, a laboratorios forenses privados, y eso entrañaba un costo, que a menudo recaía en la parte actora. La mayor parte de las veces no se pagaban los gastos de examen, lo cual menoscaba el proceso. En aquellos casos en que finalmente se abonaban, tomaba mucho tiempo a la policía recaudar la cantidad pertinente. La demora en el pago solía impedir la publicación puntual del informe, y eso hacía que el juicio se retrasara. El laboratorio de ciberdelincuencia era el único que servía a

todo el país, pero carecía del personal competente necesario. Esa falta de personal competente también afectaba gravemente a sus resultados.

119. Ghana informó de que en la actualidad había dos sentencias divergentes de su Tribunal Superior con respecto al acceso a los contenidos de un dispositivo electrónico. Conforme a una de ellas, un organismo encargado de hacer cumplir la ley no necesitaba una orden judicial para acceder al contenido de un dispositivo sospechoso; en la otra, se hacía hincapié en la necesidad de obtener una orden judicial antes de acceder al contenido. A fin de armonizar y aclarar las dos sentencias discordantes, se había remitido la cuestión a la Corte Suprema de Ghana para que adoptara una decisión al respecto.

120. La ciberdelincuencia podía, por naturaleza, atravesar varias fronteras internacionales. Por ese motivo, la información crítica necesaria para enjuiciar satisfactoriamente un caso podría encontrarse en otra jurisdicción. Ghana hizo hincapié en que lograr acceso a esa información solía ser o imposible o un proceso excesivamente lento. Si entre las partes no había un tratado de asistencia judicial recíproca, a veces no era posible obtener la información. Cuando existía un tratado de asistencia judicial recíproca, el proceso de transmisión de la información solía ser lento y burocrático, lo que provocaba demoras en la investigación y el posterior juicio de un caso.

Hungría

121. Hungría informó de que el número de víctimas del uso indebido de las tecnologías de la información y las comunicaciones había aumentado tanto nacional como internacionalmente. En general, los delincuentes preferían utilizar las aplicaciones basadas en Internet (por ejemplo, Viber, Snapchat, Messenger, WhatsApp y iMessage) frente a la tecnología basada en el Sistema Mundial de Comunicaciones Móviles, puesto que para las aplicaciones basadas en Internet no se necesitaban conocimientos especializados. Hungría consideraba que ello planteaba un desafío para la policía y otros organismos encargados de hacer cumplir la ley.

122. Hungría señaló asimismo que las tecnologías modernas de la información y las comunicaciones se utilizaban como medios para cometer delitos como el fraude en línea, la difusión de pornografía infantil en la red y el tráfico de drogas sintéticas en línea. Los medios sociales también se utilizaban para acercarse fácilmente a los niños y cometer actos de explotación sexual, en forma de fotografías o vídeos. Además, la red oscura se empleaba para adquirir, de manera ilícita y anónima, armas, drogas y documentos falsificados. Para el pago de esos productos ilícitos y peligrosos se utilizaban bitcoines. Por otra parte, si se tenía en cuenta la producción de armas o partes, la tecnología de impresión 3D podía plantear una amenaza emergente.

123. Hungría subrayó, además, que la mayoría de los delitos relacionados con las tecnologías de la información y las comunicaciones presentaban un perfil internacional y solían involucrar a más de dos países. Ello entrañaba dificultades para las autoridades cuando era necesaria una comisión rogatoria para que esos Estados intercambiaran información. Las autoridades podrían enfrentarse a dificultades al investigar delitos conexos, debido, por ejemplo, a que al usar servicios de red privada virtual resultaba más difícil determinar los datos personales válidos de los usuarios. Por lo tanto, se necesitaban más esfuerzos en la esfera de la prevención.

124. Según Hungría, los proveedores de servicios de Internet nacionales deberían cooperar estrechamente con el sector público, incluida la policía. Dado que no existían normas internacionales sobre las obligaciones de los proveedores de servicios de Internet, las autoridades nacionales deberían armonizar esas obligaciones por lo que respectaba al registro, el almacenamiento y el intercambio de información (conservación de datos) relacionados con las comunicaciones, incluidos el tipo de datos, el plazo mínimo y máximo de conservación de los datos y los pormenores de la comunicación. También debería normalizarse el requisito mínimo para que la policía pudiera enviar una solicitud a los proveedores de servicios de Internet, puesto que para tramitar una

solicitud los proveedores solían esperar más información de la que las autoridades poseían.

125. Hungría recomendaría que la designación de puntos de contacto por cada Estado miembro, prevista en el marco del Convenio sobre la Ciberdelincuencia del Consejo de Europa, se considerara una buena práctica. También propuso que se utilizaran los canales de comunicación de INTERPOL para intercambiar información.

126. Hungría informó de que el cifrado de los medios técnicos personales era útil en la prevención de la ciberdelincuencia. Sin embargo, los delincuentes utilizaban indebidamente el cifrado para ocultar su identidad y su paradero. Desbloquear el cifrado era otro desafío para la policía. Habría que concienciar acerca de ciberseguridad en los sectores público y privado. Además, a fin de mejorar la capacidad a nivel nacional era necesario actualizar la infraestructura de tecnología de la información de las instituciones y capacitar al personal de los sectores público y privado.

127. Hungría subrayó que para resolver satisfactoriamente los casos era indispensable una buena cooperación entre los distintos Estados. En Europa, Europol tenía un papel dominante en la esfera de la cooperación. El Convenio sobre la Ciberdelincuencia del Consejo de Europa podía utilizarse como una buena práctica respecto a la obtención de pruebas electrónicas de los proveedores de servicios de otros países.

128. Dado que el delito cibernético era un problema cambiante que afectaba a todos los países, Hungría consideró que a fin de combatirlo eficientemente hacía falta:

a) Aumentar al máximo el número de países que contaran con una legislación nacional adecuada y compatible en materia de ciberdelincuencia, en la que se apoyara la cooperación internacional;

b) Crear mecanismos de cooperación, confianza y competencias para compartir datos con objeto de investigar, perseguir y reducir la ciberdelincuencia;

c) Asegurarse de que no existieran refugios seguros para los delincuentes y aumentar la capacidad de las autoridades policiales y judiciales, en particular en la obtención de pruebas electrónicas.

129. Por lo que respectaba a la asistencia técnica, Hungría recordó el proyecto de estudio exhaustivo sobre el delito cibernético al señalar que había un amplio consenso con respecto a que las iniciativas de creación de capacidad para hacer frente a la ciberdelincuencia eran esenciales. Existía el Programa Mundial contra el Delito Cibernético, de la UNODC, y era importante que participaran todos los Estados Miembros. Hungría también apoyaba varios otros programas de fomento de la capacidad, como los dirigidos por el Consejo de Europa y la Unión Europea. Para Hungría, era necesario velar por que todos los proyectos de creación de capacidad estuvieran eficazmente adaptados y coordinados para evitar la duplicación, debidamente diseñados y secuenciados para satisfacer las necesidades propias de la cooperación internacional y garantizar resultados sostenibles, y eficazmente evaluados para medir su repercusión.

130. Con respecto a las opciones para fortalecer las actuales respuestas nacionales e internacionales frente a la ciberdelincuencia y proponer otras nuevas, Hungría opinó que el Convenio sobre la Ciberdelincuencia del Consejo de Europa representaba un modelo válido para la legislación nacional y un valioso marco para la cooperación internacional. El Convenio, que estaba abierto a que los países que no fueran Estados miembros del Consejo de Europa se adhirieran a él, brindaba un instrumento flexible al respecto (es decir, para el desarrollo de medidas nacionales y la promoción de la cooperación internacional). Hungría no secundaba los llamamientos a favor de que se elaborara un nuevo instrumento internacional sobre ciberdelincuencia.

131. En opinión de Hungría, el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético era y debería seguir siendo el principal proceso a nivel de las Naciones Unidas en materia de ciberdelincuencia, al menos hasta 2021. El Grupo de Expertos había dado resultados, por ejemplo, respecto a las reformas legislativas (basadas en las normas internacionales vigentes) y a la creación de

capacidad. En los últimos seis años se habían registrado notables avances en cuanto a las reformas legislativas, en particular cuando los países habían hecho uso de las normas internacionales vigentes. Muchas organizaciones habían establecido programas de creación de capacidad. Estos esfuerzos deberían continuar y seguir ampliándose.

132. Hungría sugirió que los Estados Miembros apoyaran a la UNODC en la adopción de las siguientes medidas contra la amenaza que planteaba el delito cibernético:

a) Reforzar las competencias policiales y de aplicación de la ley mediante capacitación general y especializada;

b) Prestar asistencia técnica en los países en desarrollo;

c) Analizar las deficiencias en la cooperación internacional a fin de determinar las esferas prioritarias;

d) Prestar apoyo a campañas de sensibilización pública para reforzar la prevención del delito y para lograr que la sociedad civil y las empresas cooperaran con las entidades encargadas de hacer cumplir la ley;

e) Fortalecer los mecanismos operacionales existentes, como la Red 24/7;

f) Recopilar datos sobre las amenazas que planteaba la ciberdelincuencia;

g) Actuar como un repositorio de mejores prácticas y estudios de casos respecto de la lucha contra el delito cibernético.

India

133. La India se refirió al constante aumento de la ciberdelincuencia, que había planteado nuevas cuestiones y desafíos en la tarea de hacer cumplir la ley. La ciberdelincuencia difería significativamente de los delitos tradicionales en cuanto a su naturaleza, alcance, medios, pruebas y actividades; por ello, el intercambio de información en tiempo real o casi real resultaba esencial para lograr, mediante la recopilación de pruebas, someter a los ciberdelincuentes a la acción de la justicia. Los delitos relacionados con la ciberdelincuencia eran técnicamente complejos y jurídicamente intrincados. El ciberespacio y la ciberdelincuencia no tenían límites físicos y, por lo tanto, la cooperación internacional era fundamental, entre otras cosas, para la investigación, la recopilación de datos y pruebas, y el castigo.

134. La India comunicó que, de acuerdo con su Oficina Nacional de Registro de la Delincuencia, se habían registrado 9.622 delitos cibernéticos en 2014, 11.592 en 2015 y 12.317 en 2016. En 2016 el 48,6 % de los casos de ciberdelincuencia comunicados tenían que ver con ganancias ilícitas (5.987 de 12.317), seguidos de actos de venganza (8,6 %, es decir, 1.056 casos) e insultos contra la modestia de las mujeres (5,6 %, es decir, 686 casos).

135. La India se refirió también al marco jurídico e institucional nacional en materia de ciberdelincuencia al señalar que la Ley de Tecnología de la Información de 2000, en su versión modificada en 2008, y el Código Penal de la India sentaban el marco jurídico con el que responder al comercio electrónico, la ciberseguridad, la ciberdelincuencia y el ciberterrorismo. Las leyes nacionales son bastante amplias y abarcan la mayoría de las cuestiones relacionadas con la ciberdelincuencia.

136. La India señaló asimismo que diversos tipos de uso indebido de las tecnologías de la información y las comunicaciones, en forma de delitos cibernéticos “básicos”, así como la ciberdelincuencia asistida por las tecnologías de la información y las comunicaciones, planteaban desafíos variables que era necesario encarar. El uso indebido de las tecnologías de la información y las comunicaciones comprendía las intrusiones en los sitios web y sus desfiguraciones (*defacement*), los virus o código malicioso, los ataques de negación de servicios y los ataques de negación de servicios distribuidos, la piratería informática, el *phishing*, el ciberterrorismo, la pornografía infantil, la “sextorsión”, el robo de identidad, el ciberacoso y hostigamiento, las noticias

falsas y la propaganda, las apuestas ilícitas, la venta de medicamentos y fármacos falsos, el ciberespionaje, etc.

137. La India señaló que los delitos cibernéticos se cometían utilizando modernos instrumentos de las tecnologías de la información y las comunicaciones, como programas maliciosos ("*malware*"), *botnets*, enrutamiento de cebolla e incluso teléfonos móviles corrientes empleados con fines de ingeniería social.

138. La India se refirió a los siguientes desafíos en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos:

a) El uso de numerosas variantes de programas maliciosos y *botnets*, que permitía a los delincuentes evitar controles técnicos como los programas antivirus y los filtros de Internet, así como ser detectados por las entidades encargadas de hacer cumplir la ley;

b) El uso de esas tecnologías con ocultamiento, el anonimato, el poder computacional y la imposibilidad de rastrear la fuente o el autor del delito;

c) El hecho de que los servicios de red privada virtual permitieran comunicarse de forma anónima por Internet;

d) La multiplicidad de instrumentos que permitían a los delincuentes mantenerse anónimos en línea o ilocalizables. De esos instrumentos, los *botnets* planteaban el mayor problema por diversas razones;

e) El hecho de que la lucha contra el delito cibernético exigiera conocimientos jurídicos especializados, aptitudes investigadoras, instrumentos forenses e ingenio analítico;

f) Respecto a las dificultades jurídicas, el hecho de que la naturaleza transnacional de la ciberdelincuencia entrañara complejidad jurisdiccional, lo cual dificultaba la investigación y el enjuiciamiento. La falta de armonización legislativa entre un país y otro planteaba dificultades en la investigación y el enjuiciamiento de los delitos de ciberterrorismo.

139. La India, centrándose en los problemas a nivel internacional que obstaculizaban la cooperación en la lucha contra el uso delictivo de las tecnologías de la información y las comunicaciones, se refirió a lo siguiente:

a) El tiempo era fundamental en las investigaciones en materia de ciberdelincuencia y, por ende, había de definirse un plazo para el suministro de pruebas digitales en caso de cooperación multilateral entre Estados;

b) Los tratados de asistencia judicial recíproca se centraban principalmente en los escenarios posteriores al delito, si bien, a diferencia de lo que ocurría con los delitos tradicionales, el rápido intercambio de información era esencial para prevenir la ciberdelincuencia. También era precisa la cooperación internacional en la esfera de la prevención del delito cibernético;

c) Los tratados de asistencia judicial recíproca carecían de una cláusula para satisfacer las necesidades propias de los casos de emergencia, que era un requisito fundamental para hacer frente a los delitos cibernéticos. Ese aspecto debía examinarse;

d) La cooperación internacional en materia de ciberdelincuencia era esencial dado el uso generalizado de las tecnologías de control y mando, los *botnets* y las tecnologías de la red profunda;

e) Las leyes sobre privacidad obstaculizaban el intercambio de información.

Irán (República Islámica del)

140. Con respecto a los desafíos en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, la República Islámica del Irán comunicó, como primer problema, el incumplimiento por parte de los proveedores de

Internet y redes sociales extranjeros. Internet y los medios sociales habían contribuido enormemente a mejorar la vida humana. Sin embargo, la ubicuidad y la transferibilidad de la telecomunicación sin fisuras que se producía a través de Internet y los medios sociales habían hecho que los delincuentes, especialmente los grupos delictivos organizados, utilizaran cada vez más esas tecnologías con fines delictivos. Los proveedores de servicios de Internet y redes sociales desempeñaban un papel indispensable para prevenir y combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, concretamente en la esfera de la recopilación y conservación de pruebas electrónicas, así como de la aplicación de la ley.

141. Para la República Islámica del Irán, una respuesta justa y resiliente dependería en gran medida de la regulación de las actividades en los medios sociales. Las actividades en los medios sociales que eran propiedad del sector privado iraní estaban bien reguladas por las autoridades nacionales, en consonancia con lo dispuesto en la Ley Procesal de Delitos Informáticos. Las fuerzas del orden podían detectar actividades delictivas en el ciberespacio, reunir y conservar pruebas electrónicas e investigar y enjuiciar eficazmente la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Sin embargo, dada la naturaleza extraterritorial de la ciberdelincuencia, las autoridades se enfrentaban a graves dificultades al enjuiciar delitos cometidos mediante el uso de servidores situados en otros países y que eran propiedad extranjera, ya fuera pública o privada. En la mayoría de los casos, los servicios extranjeros de redes sociales no cooperaban en asuntos penales. El incumplimiento, por parte de esas entidades, de las solicitudes de cooperación de los Estados planteaba un problema para prevenir y combatir eficazmente los delitos y ponía en peligro el estado de derecho en los planos nacional e internacional.

142. Con respecto a las medidas coercitivas unilaterales, la República Islámica del Irán, situada en una región afectada por la delincuencia organizada, comunicó impedimentos internacionales a la cooperación en materia de asuntos penales a nivel internacional, en particular en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Las medidas coercitivas unilaterales, que actuaban en detrimento de una respuesta colectiva a esos delitos, impedían que los países cooperaran con las fuerzas del orden iraníes en la investigación y el enjuiciamiento de los delitos, en particular, los cometidos mediante la utilización de las tecnologías de la información y las comunicaciones, así como en la transferencia de los instrumentos tecnológicos necesarios para conservar las pruebas electrónicas y realizar exámenes forenses digitales. Las medidas coercitivas unilaterales, que constituían una violación flagrante de los principios fundamentales del derecho internacional consagrados en la Carta de las Naciones Unidas, no solo ponían trabas a la cooperación eficaz en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, sino que también debilitaban el estado de derecho, y esto envalentonaba a los delincuentes en el ejercicio de sus actividades ilícitas. La eliminación de los obstáculos internacionales seguía siendo vital, no solo para luchar eficazmente contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, sino también para garantizar la seguridad colectiva de los Estados. La República Islámica del Irán estaba decidida a luchar contra la delincuencia organizada. Apoyaba la cooperación internacional contra el delito cibernético facilitada por la UNODC y ponía de relieve la necesidad de reforzar la asistencia técnica en esa esfera.

143. En relación con la falta de un marco internacional inclusivo, la República Islámica del Irán destacó la necesidad de contar con un marco jurídico internacional sobre ciberdelincuencia. En la actualidad, la falta de un marco internacional sólido e inclusivo sobre ciberdelincuencia seguía siendo un problema en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. La naturaleza del delito cibernético requería una respuesta adaptada al contexto, resiliente y colectiva, por conducto de un instrumento internacional, teniendo en cuenta la necesidad de mantener el ritmo al que se desarrollaban la tecnología y los nuevos *modus operandi* de los grupos delictivos organizados. Los instrumentos existentes en materia de ciberdelincuencia, al haber sido elaborados por un número limitado de

Estados, no reunían los requisitos necesarios para una respuesta de esa índole y eso, a su vez, hacía que fueran inaplicables a nivel internacional.

144. La República Islámica del Irán encomió y apreció la amplia y valiosa labor de la UNODC, en particular, del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético. La República Islámica del Irán afirmó que seguía apoyando la labor de la UNODC en ese empeño y que creía que la aprobación de una convención universal sobre el delito cibernético bajo los auspicios de las Naciones Unidas redundaría en beneficio de los Estados y mitigaría los desafíos en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

145. Por lo que respectaba al marco jurídico sobre ciberdelincuencia, en la República Islámica del Irán los delitos tradicionales facilitados o permitidos por el uso del ciberespacio eran punibles con arreglo al Código Penal Islámico. Sin embargo, la Asamblea Consultiva Islámica (Parlamento) había redactado y promulgado legislación cibernética a fin de prevenir y combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, en particular la ciberdelincuencia, de manera eficiente y resiliente. La legislación también abarcaba las pruebas electrónicas, dada su función indispensable en el enjuiciamiento del delito cibernético.

146. Desde la perspectiva de las leyes penales sustantivas, la República Islámica del Irán se refirió a la Ley de Comercio Electrónico, de 2004. Con arreglo a esa Ley, se reconocieron las medidas de protección de los dispositivos y contratos electrónicos con respecto a los secretos comerciales y se penalizaron el uso indebido de datos personales, la vulneración de los derechos del consumidor y la divulgación de información comercial clasificada en transacciones electrónicas, así como el fraude y la falsificación informáticos. Se informó de que la Ley de Delitos Informáticos de 2009 incluía disposiciones relativas a la penalización y la responsabilidad de las personas jurídicas. Con arreglo a esa Ley se penalizaron, entre otras cosas, el acceso a los datos y sistemas informáticos sin autorización, la difusión de contenido obsceno, los atentados contra la integridad y la confidencialidad de los datos, y el robo y fraude informáticos. Los delitos se castigaban con una multa y una pena de prisión de hasta 15 años. En el artículo 26 se establecía como agravante la comisión de delitos cibernéticos de manera organizada, a gran escala o contra los sistemas informáticos de la administración pública. La Ley se estaba examinando actualmente para adaptarse a los nuevos *modus operandi* de los delincuentes y para brindar un marco jurídico resiliente a las autoridades encargadas de hacer cumplir la ley.

147. Desde la perspectiva del derecho procesal, la República Islámica del Irán se refirió a la Ley Procesal de Delitos Informáticos, que antes formaba parte de la Ley de Delitos Informáticos de 2009, y que posteriormente se incorporó a la Ley de Procedimiento Penal con modificaciones menores. Ese instrumento legislativo abarcaba cuestiones como la jurisdicción, las dependencias especializadas para la investigación, el enjuiciamiento de los delitos cibernéticos y las condiciones y los procedimientos de búsqueda e incautación de pruebas electrónicas, datos y sistemas informáticos. La Ley velaba por el respeto de las garantías procesales y la protección de la privacidad. Con arreglo a los artículos 671 y 672, las órdenes judiciales de búsqueda e incautación de datos únicamente estaban permitidas cuando existieran motivos sólidos y razonables que justificaran esa orden, que debería ejecutarse en presencia del propietario legal. Conforme a lo dispuesto en el artículo 679, quedaba prohibida toda incautación que entrañara daños para la propiedad o entorpeciera el servicio público.

Iraq

148. El Iraq observó que el uso de Internet era una de las características de la civilización moderna y una medida del desarrollo, la integración en la civilización humana y la interacción con otros países. Se había producido, por consiguiente, una revolución en los métodos de intercambio científico y cultural. Internet se había

convertido en un enorme canal de conocimientos y había contribuido así a la vinculación y cohesión de las sociedades y personas más allá de las fronteras geográficas, los determinantes políticos y sociales y las doctrinas intelectuales; como también había contribuido a la convergencia de las civilizaciones y al intercambio de ideas entre distintas nacionalidades, idiomas y religiones. Ello hacía que se considerara por qué valores y principios se debería regir el contenido de Internet: un tema que seguía resultando importante y polémico. Aunque en los países en desarrollo se encontraba un pequeño porcentaje de los usuarios de Internet en el mundo, la cuestión del contenido era de gran importancia para ellos, dada la repercusión que tenía sobre sus sociedades. Si bien uno de los valores de Internet era la igualdad y libertad, la privacidad de las sociedades de los países en desarrollo exigía que los Gobiernos tuvieran en cuenta esa particularidad e intentaran protegerlas de múltiples orientaciones y culturas.

149. El Iraq subrayó que esa convergencia de los pueblos también repercutía en la globalización de la delincuencia y las conductas delictivas, incluidos los delitos que afectaban a las sociedades conservadoras en los países en desarrollo. Por lo tanto, hacía falta crear reglamentos sobre la ética de Internet acordes con las particularidades de cada comunidad. Así, la elaboración de unos estatutos determinaría el contenido de Internet aplicable a cada país o zona según las normas éticas correspondientes, y no estaría necesariamente a disposición de todos.

150. El Iraq puso de relieve que, en el decenio anterior, el uso de aplicaciones en línea se había propagado exponencialmente. Por ello, era necesario organizarlas y regularlas. Algunas aplicaciones recientes (de entretenimiento o juegos) exigían a sus abonados que les permitieran acceder a una serie de datos personales. Dado que el nivel de acceso a la información disponible en una red determinaba el nivel de privacidad de los usuarios en esa misma red, el Iraq alentaba a los diseñadores y promotores de las aplicaciones a que fijaran normas conforme a las cuales se les exigiera demostrar el propósito de acceder a determinada información o dispositivos. Otro enfoque consistiría en que hubiera voluntarios que evaluaran las aplicaciones sobre la base de normas convenidas, a fin de aumentar la confianza en las aplicaciones apropiadas y reducirla con respecto a las maliciosas.

151. El Iraq comunicó que se sabía que las noticias se propagaban rápidamente por Internet a un público amplio que podría no ser capaz de verificar su fuente o podría no tener interés en hacerlo. Se debería alentar a las empresas a tratar las noticias de manera precisa y objetiva y a no publicar noticias o vídeos falsos que pudieran avivar el odio entre las comunidades. También podría ser preciso, especialmente en la actualidad, reducir las fuentes de videos y medios auditivos y escritos que incitaran al odio. También sería útil aumentar la colaboración entre los patrocinadores de los medios de comunicación y sociales y los equipos voluntarios de evaluación que analizaban las noticias y examinaban su credibilidad.

152. En relación con los riesgos en línea para los niños, el Iraq señaló que la sociedad de la información brindaba un mundo digital instantáneo con tan solo pulsar un ratón. A través de las computadoras o los dispositivos móviles con acceso a Internet se podía consultar un volumen inaudito de servicios e información. Los obstáculos que planteaban, por ejemplo, los gastos de los dispositivos y de acceso a Internet se estaban reduciendo rápidamente. Esos avances brindaban a los niños y jóvenes oportunidades sin precedentes de convertirse en “ciudadanos digitales”, en un mundo en línea carente de fronteras o límites. Entre los riesgos y vulnerabilidades relacionados con el uso de Internet a los que se enfrentaban los niños y jóvenes al estar en línea figuraban los siguientes:

a) Exposición a contenido ilícito y dañino, como pornografía, apuestas, sitios que incitaban a autolesionarse, escenas de violencia, terrorismo y otros contenidos inapropiados, así como al contacto con otros usuarios. En la mayoría de los casos, los operadores de sitios web con contenido de esa índole no adoptaban medidas eficaces para restringir el acceso a los niños;

b) Recepción de correos basura y anuncios publicitarios que promocionaban productos orientados a determinada edad o intereses;

c) Uso compulsivo y excesivo de Internet y juegos en línea;

d) Intimidación, acoso, amenazas y extorsión;

e) Exposición a radicalización y racismo y otros discursos e imágenes discriminatorios;

f) Declaraciones falsas sobre la edad de una persona;

g) Uso indebido de datos personales y divulgación de información personal, con el consiguiente riesgo de padecer daños físicos y vulneración de los derechos propios o ajenos, mediante el plagio y la publicación de contenido (especialmente de los medios) sin permiso, incluidas fotografías inapropiadas.

153. Centrándose en las cuestiones de seguridad pública, el Iraq subrayó que las grandes empresas de Internet ofrecían estupendos servicios y oportunidades para el desarrollo social y económico. Las plataformas en línea servían para el desarrollo socioeconómico solo cuando los usuarios representaban su verdadera identidad. En cambio, cuando recurrían al anonimato o a un nombre falso, lo cual era muy común en los medios sociales, podrían estar utilizando indebidamente esos servicios y realizar actividades delictivas, como difundir discursos de odio, ideologías terroristas y mensajes de amenaza o chantaje. Se trataba de un difícil reto en materia de seguridad pública para los Gobiernos de los países en desarrollo, especialmente cuando carecían de tecnologías de alto nivel y trataban de obtener la cooperación de las empresas de Internet. Esas empresas podían recabar información general y personal de sus clientes como parte del proceso de gestión de sus cuentas, con la que podían vigilar sus ubicaciones geográficas, números de teléfono y otra información útil, y podrían impedir la comisión de delitos y salvar vidas. Ello llevaba a exhortar a las partes interesadas a asumir, en estrecha colaboración, su parte de responsabilidad con objeto de resolver esos problemas y garantizar unos servicios continuos y más seguros para cumplir los Objetivos de Desarrollo Sostenible.

154. El Iraq también se refirió a otros desafíos en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, entre los que figuraban la falta de una convención mundial contra el delito cibernético; la dificultad para comprender las pruebas digitales, o parte de ellas, y la facilidad para destruirlas o hacerlas desaparecer; el hecho de que la ciberdelincuencia trascendiera las fronteras geográficas, sumado a la distancia geográfica entre el delincuente y la víctima; la falta de una capacitación y creación de capacidad suficientes para que las autoridades competentes combatieran el delito cibernético; el hecho de que las organizaciones no gubernamentales y otras entidades gubernamentales a veces no utilizaran debidamente la experiencia y los conocimientos técnicos especializados en la investigación de la ciberdelincuencia; la falta de una infraestructura electrónica adecuada para luchar contra la ciberdelincuencia; y la dificultad para limitar o restringir la manera en que se cometía el delito cibernético.

155. El Iraq llegó a la conclusión de que había una necesidad creciente y urgente de intensificar la cooperación entre las partes interesadas para garantizar un futuro digital seguro.

Irlanda

156. Irlanda se refirió al estudio exhaustivo sobre el delito cibernético, en el que se había señalado que había un amplio consenso con respecto a que las iniciativas de creación de capacidad para hacer frente a la ciberdelincuencia eran esenciales. De hecho, en la quinta reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, hubo un acuerdo generalizado respecto de que, en la actualidad, la falta de capacidad suficiente planteaba el que quizás fuera el más importante desafío para hacer frente eficazmente a la ciberdelincuencia.

157. Irlanda destacó que como resultado de que cualquier delito podía entrañar un elemento cibernético, sobre todo respecto a las pruebas electrónicas, surgía un reto

importante en cuanto a la creación de capacidad. Era, por lo tanto, fundamental que todos los investigadores, fiscales y jueces poseyeran los conocimientos especializados pertinentes en esa esfera. El desarrollo de los profesionales especialistas, cuando procediera, también revestía importancia. Ese reto se veía acentuado por el hecho de que, dado el carácter internacional de la ciberdelincuencia, la falta de capacidad suficiente en un Estado podía menoscabar la capacidad para combatir un delito no solo en ese Estado, sino en cualquier otro.

158. A fin de superar esos retos, Irlanda señaló que era importante continuar y ampliar los programas de creación de capacidad en los planos nacional e internacional. Esos proyectos de creación de capacidad debían estar eficazmente adaptados y coordinados para evitar la duplicación y asegurar su sostenibilidad. También deberían estar debidamente diseñados con respecto a los requisitos específicos de los ordenamientos jurídicos discrepantes de los Estados y las necesidades en materia de cooperación internacional. Por último, deberían ser evaluados de manera estricta a fin de fundamentar la elaboración de futuros proyectos.

159. Irlanda reconoció el valor del foro que el Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético brindaba para el intercambio de conocimientos y experiencias en relación con los desafíos planteados por el delito cibernético. En particular, señaló que la naturaleza del Grupo de Expertos como un foro de expertos, y no político, había sido fundamental para su éxito. Por ello, Irlanda creía que el Grupo de Expertos debería seguir siendo el principal proceso a nivel de las Naciones Unidas en materia de ciberdelincuencia.

160. Asimismo, Irlanda señaló que las principales dificultades encontradas en relación con la ciberdelincuencia no tenían que ver con el marco jurídico internacional en esa esfera. Por lo tanto, confirmó que no secundaba las propuestas de elaboración de un nuevo instrumento internacional sobre ciberdelincuencia. Como primer instrumento internacional vinculante en la lucha contra la ciberdelincuencia, el Convenio sobre la Ciberdelincuencia del Consejo de Europa había demostrado ser, por un lado, flexible al entorno tecnológico en constante cambio y, por otro, de alcance mundial. El carácter mundial del Convenio quedaba de manifiesto con la participación de 63 Estados partes de los 5 grupos regionales de las Naciones Unidas, y con que un número considerable de Estados que no eran partes en el Convenio hubieran promulgado leyes contra la ciberdelincuencia tomando como modelo el Convenio. En ese sentido, las disposiciones sustantivas del Convenio se habían incorporado en gran medida al derecho irlandés, e Irlanda se había comprometido a ratificar el Convenio lo antes posible.

161. Irlanda manifestó su pleno apoyo a los esfuerzos que se estaban realizando para negociar un segundo protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa respecto de una mayor cooperación internacional, que mejoraría aún más el Convenio y ayudaría a asegurar que este siguiera siendo el instrumento internacional más importante en materia de ciberdelincuencia.

Israel

162. Israel subrayó que, habida cuenta de que las plataformas de propiedad privada de las empresas de tecnologías de la información también podían utilizarse para actividades delictivas, uno de los principales desafíos a los que se enfrentaban los Estados en la actualidad era la interacción entre el Estado y las empresas privadas. En ese sentido, era preciso considerar un marco apropiado y equilibrado, por una parte, para permitir que las empresas prestaran servicios fiables a sus clientes, al mismo tiempo que mantenían su privacidad y libertad de expresión y promovían la innovación y, por otra, para cooperar adecuadamente con las autoridades encargadas de hacer cumplir la ley en los casos de actividad delictiva.

Italia

163. Italia comunicó que la Policía Nacional Italiana, por conducto del Servicio de Policía Postal y de Comunicaciones, era la encargada de prevenir y combatir la ciberdelincuencia. El Centro Nacional 24 Horas contra los Delitos relativos a la Tecnología de la Información y para la Protección de las Infraestructuras Críticas, establecido dentro del Servicio de Policía Postal y de Comunicaciones, se dedicaba exclusivamente a prevenir y combatir los delitos de la tecnología de la información (ya sean de carácter común, organizado o terrorista) cometidos contra las infraestructuras críticas. Cumplía satisfactoriamente su cometido mediante una vigilancia continua de Internet. El Centro Nacional 24 Horas contra los Delitos relativos a la Tecnología de la Información y para la Protección de las Infraestructuras Críticas prestaba servicios de protección cibernética sobre la base de los acuerdos concertados entre el Departamento de Seguridad Pública y las entidades que gestionaban las infraestructuras críticas (alianza público-privada). El Centro también incluía el punto de contacto italiano en caso de emergencias técnicas y operacionales relacionadas con actos delictivos transnacionales.

164. Por lo que respectaba al ciberterrorismo, Italia comunicó que el Servicio de Policía Postal y de Comunicaciones se encargaba de prevenir y combatir la incitación en línea al terrorismo yihadista, sobre todo mediante la vigilancia de Internet con el apoyo de mediadores lingüísticos y culturales y en colaboración con la Dirección Central de la Policía de Prevención y la División General de Investigaciones y Operaciones Especiales de la Policía. Además, sin perjuicio de las competencias de la Policía Nacional, el Cuerpo de Carabinieri y la Guarda di Finanza, que se ocupaban de las actividades de investigación en la esfera del terrorismo y la subversión, el Servicio de Policía Postal y de Comunicaciones actualizaba constantemente la lista de sitios web utilizados con fines terroristas. Asimismo, la Guardia di Finanza, por conducto de la Dependencia Especial contra Fraudes Tecnológicos, detectaba, prevenía y combatía los delitos cometidos haciendo uso de instrumentos cibernéticos en materia de evasión de impuestos, delitos de aduanas, fraudes relacionados con los recursos de la Unión Europea, delitos monetarios y falsificaciones.

165. A nivel europeo, el Servicio de Policía Postal y de Comunicaciones actuaba como punto de contacto nacional para la Unidad de Notificación de Contenidos de Internet de Europol, encargada de recibir los informes de los Estados Miembros acerca del contenido de la propaganda terrorista yihadista en línea.

166. En relación con el sector bancario, y conforme a una directiva del Ministro del Interior, al Servicio de Policía Postal y de Comunicaciones le había sido encomendada la tarea de prevenir y combatir la ciberdelincuencia cuando se emplearan técnicas concretas de *phishing*, piratería informática o tecnologías de programas o equipos informáticos a fin de robar, reproducir y utilizar fraudulentamente identidades digitales, códigos para utilizar servicios de banca en línea y tarjetas de pago en transacciones electrónicas.

167. Con respecto a las criptomonedas, Italia señaló que a menudo se utilizaban como medio de pago para adquirir bienes y servicios. Esas transacciones se caracterizaban por el anonimato tanto de los autores como de los beneficiarios reales, lo alentaba su uso con fines ilícitos (por ejemplo, en el marco del *phishing* y los criptovirus de programas secuestradores).

168. Italia afirmó que, dentro del Servicio de Policía Postal y de Comunicaciones, se había establecido un centro nacional para combatir la pornografía infantil en línea. El centro actualizaba continuamente una lista negra que se transmitía a los proveedores de servicios de Internet de modo que estos pudieran impedir que los usuarios de Internet en Italia accedieran a espacios virtuales que contuvieran materiales en línea de abuso sexual infantil procedentes de otros países. El centro también dependía de la cooperación de todos los agentes institucionales y sociales que participaban en la educación y la protección de los menores, a fin de aplicar estrategias comunes contra esos fenómenos e investigar y desarrollar nuevas técnicas en apoyo de las

investigaciones. Las innovadoras metodologías de investigación adoptadas por el Servicio de Policía Postal y de Comunicaciones se basaban en las más sofisticadas técnicas encubiertas, con objeto de desmantelar los sistemas de anonimización y permitir la identificación de los sujetos involucrados y los menores de los que se hubiera abusado. Las investigaciones también iban orientadas a las redes sociales, en las que se observaban nuevas formas de engaño y episodios de ciberacoso, así como delitos de difamación en línea (sobre todo contra personas con responsabilidades institucionales), acoso criminal, hostigamiento, amenazas e incitación al odio.

Japón

169. El Japón se centró, en primer lugar, en una dificultad específica que emanaba de la naturaleza de la ciberdelincuencia. Los delitos cibernéticos eran extremadamente anónimos y apenas dejaban huellas. Además, la ciberdelincuencia no tenía limitaciones territoriales ni temporales y podría causar daños instantáneamente a innumerables víctimas. Los delincuentes podían, por lo tanto, perpetrar fácilmente el delito cibernético explotando a los países vulnerables que carecían de contramedidas eficaces y utilizar a esos países como base para realizar actividades cibernéticas delictivas contra víctimas de todo el mundo. Por consiguiente, un desafío común para la comunidad internacional era colmar esa brecha en materia de capacidad de modo que todo país dispusiera de medidas contra la ciberdelincuencia suficientes y apropiadas que no permitieran a los delincuentes margen de maniobra.

170. Para el Japón, ese desafío se veía agravado por dos aspectos: la falta de marcos jurídicos y la falta de fomento de la capacidad. La falta, en algunos Estados Miembros, de marcos jurídicos sólidos de derecho sustancial y procesal con los que hacer frente al delito cibernético suponía un gran problema. Por ejemplo, los países que carecían de legislación suficiente para penalizar la creación de virus informáticos o los países sin una legislación que permitiera la conservación de datos de Internet planteaban graves dificultades en la lucha contra la ciberdelincuencia. Para hacer frente a ese desafío, la comunidad internacional debería ayudar a los Estados Miembros a promulgar nuevas leyes que permitieran hacer frente a las formas nuevas y emergentes de ciberdelincuencia y resistir el paso del tiempo.

171. Según el Japón, la manera más amplia y eficaz en función del costo de lograr ese objetivo sería utilizar los marcos jurídicos internacionales vigentes. Esto no solo evitaría que se duplicaran las labores, sino que también permitiría a los Estados Miembros promulgar legislación con las normas que ya estuvieran ampliamente aceptadas. Se colmaría así la brecha entre los Estados Miembros y, además, se facilitaría la cooperación internacional (por ejemplo, el principio de doble incriminación se cumpliría mejor entre Estados Miembros con marcos jurídicos similares). En ese sentido, el Convenio sobre la Ciberdelincuencia del Consejo de Europa había sido ampliamente aceptado por la sociedad internacional y brindaba un punto de partida común. La promulgación de leyes en consonancia con dicho Convenio había demostrado ser eficaz en el Japón. Por ejemplo, el delito de “creación de registros electromagnéticos de comandos no autorizados” (artículo 168-2 del Código Penal), aprobado en 2011 en consonancia con el Convenio, se había aplicado con éxito a las formas nuevas y emergentes de delincuencia cibernética, como la creación de programas informáticos secuestradores, que no se habían previsto en el momento de la promulgación.

172. El Japón subrayó que, incluso si se dispusiera de marcos jurídicos sólidos, la falta de capacidad por parte de los organismos encargados de hacer cumplir la ley y el poder judicial para hacer uso de ellos socavaría gravemente los esfuerzos por combatir la ciberdelincuencia. La capacidad de las entidades encargadas de hacer cumplir la ley para detectar, investigar y reunir pruebas electrónicas resultaba indispensable en ese sentido. El poder judicial también debía entender los *modus operandi* de la ciberdelincuencia y comprender como era debido las pruebas electrónicas, con miras a decidir adecuadamente respecto de la admisibilidad y credibilidad de esas pruebas. El Japón entendía que, a nivel de la comunidad internacional, la prestación de fomento de la

capacidad y asistencia técnica a los Estados Miembros que la necesitaban seguía siendo insuficiente.

173. El Japón comunicó que había venido proporcionando programas de creación de la capacidad a los países que la necesitaban mediante, entre otras cosas, programas de capacitación específicos para cada país, algunos operados por la Agencia de Cooperación Internacional del Japón, y el diálogo sobre ciberdelincuencia entre el Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente y la Asociación de Naciones de Asia Sudoriental (ASEAN) y el Japón. Un desafío común era lograr que los países receptores pudieran proseguir de manera autónoma y sostenible sus propias iniciativas de fomento de la capacidad. En ese sentido, el Gobierno del Japón venía cooperando desde 2006 con el Complejo Mundial de INTERPOL para la Innovación, a fin de prestar a los países la asistencia necesaria para alentar sus propias iniciativas de fomento de la capacidad.

174. El Japón puso de relieve la necesidad de proseguir las deliberaciones de los expertos y recalcó que la manera más eficaz de determinar los retos relacionados con la legislación y la falta de capacidad para prestar asistencia técnica en la lucha contra la ciberdelincuencia era escuchar las opiniones y experiencias de los expertos. Los expertos podían presentar una imagen actualizada de la cuestión del delito cibernético teniendo en cuenta su naturaleza cambiante, así como los desafíos nuevos y emergentes. Los debates entre expertos permitirían comprender mejor toda la magnitud del problema, con miras a determinar dónde debería centrar sus esfuerzos la comunidad internacional.

175. El Japón se refirió al Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético en Viena, que reunía a expertos pertinentes de todo el mundo y proporcionaba el lugar ideal para examinar y determinar las tendencias actuales, los desafíos y el camino a seguir. En la actualidad, el Grupo de Expertos debatía anualmente los temas pertinentes, conforme a un plan de trabajo plurianual aprobado por consenso entre todos los Estados Miembros. Estaba previsto que el Grupo prosiguiera su labor y realizara un balance en 2021. Ese ejercicio permitiría a la comunidad internacional determinar los numerosos desafíos, así como las medidas que se habían de adoptar. Todo debate sobre ciberdelincuencia debía basarse en aportaciones concretas de expertos y fundamentadas en pruebas. Por lo tanto, los resultados del Grupo de Expertos deberían considerarse como base para futuras deliberaciones. El Gobierno del Japón creía firmemente que las deliberaciones sobre ciberdelincuencia deberían celebrarse dentro del Grupo de Expertos, en Viena. En otras palabras, todo movimiento que entorpeciera los esfuerzos del Grupo de Expertos, por ejemplo, trasladar las deliberaciones sobre ciberdelincuencia fuera de Viena, a un foro en el que participaran pocos expertos, debilitaría gravemente la capacidad de la comunidad internacional para combatir la ciberdelincuencia.

Jordania

176. Jordania enumeró las siguientes cuestiones como principales problemas en relación con la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines ilícitos o delictivos:

a) La existencia de *software* libre y programas que ocultaban las identidades de los usuarios y dificultaban la tarea de rastrearlos y detectarlos;

b) La disponibilidad de la información y la facilidad para obtenerla, así como la posibilidad de adquirir conocimientos y experiencia sobre el uso de instrumentos delictivos a partir de múltiples sitios web gratuitos y ampliamente disponibles;

c) La red oscura, que constituía un terreno fértil para las actividades ilícitas, como la contratación de personas para cometer un asesinato, el tráfico de drogas, la trata de personas y la explotación infantil, y que hacía que vigilar y supervisar esos sitios web y usuarios fuera una tarea difícil, dado el uso de cifrado para impedir que se detectara la identidad de los usuarios;

d) La lentitud de los procedimientos y del intercambio de información en los casos de ciberdelincuencia que tenían lugar en varias jurisdicciones, sobre todo teniendo en cuenta que la ciberdelincuencia requería unos procedimientos y una tramitación rápidos;

e) La falta de respuesta y cooperación en materia de intercambio de información con los organismos encargados de hacer cumplir la ley por parte de algunas plataformas de medios sociales;

f) La necesidad de creación de capacidad mediante programas de capacitación internacionales y el intercambio de experiencias con los países desarrollados en materia de ciberdelincuencia.

Líbano

177. El Líbano informó de que 2018 había sido un año de mucha actividad en la lucha contra la utilización de las tecnologías de la información con fines delictivos a nivel del poder ejecutivo, la autoridad parlamentaria y el poder judicial. En el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT) correspondiente a 2018, el Líbano ocupó el 124º puesto mundial, mientras que con respecto a su tasa de uso de Internet ostentó el 65º puesto (Índice de la UIT de Desarrollo de las TIC correspondiente a 2017).

178. El Gobierno del Líbano asignaba gran importancia a la cuestión de la ciberseguridad. En una declaración ministerial se hizo referencia explícita a la mejora de los procedimientos y medidas para proteger el ciberespacio y la infraestructura de la información libaneses, así como los datos personales de particulares e instituciones, que el Gobierno tenía la intención de cumplir junto con un proyecto de gobierno electrónico titulado “Gobierno Digital”. Se había establecido un nuevo ministerio (Ministerio de Estado para Asuntos Tecnológicos) dentro del nuevo Gobierno.

179. Además, el Primer Ministro adoptó una decisión a finales de 2018 para formar un equipo nacional de ciberseguridad en el que participaran representantes de los ministerios y de los departamentos pertinentes. Se encomendó al equipo que formulara una estrategia nacional de ciberseguridad en el Líbano y que estableciera una autoridad nacional para hacer frente a esa cuestión. La estrategia nacional que se está elaborando incluye cinco cuestiones fundamentales. Tras un período de preparación, las labores relativas a ese plan comenzaron el 15 de noviembre de 2018, y estaba previsto que finalizaran dentro de los dos meses siguientes.

180. El Líbano también informó de que las comisiones parlamentarias, entre ellas la Comisión de Tecnología de la Información y la Comisión de Información y Comunicaciones, habían celebrado varias sesiones parlamentarias para evaluar la situación actual y formular recomendaciones.

181. En el plano legislativo, la Ley Núm. 81/2018, relativa a las transacciones electrónicas y la protección de los datos personales, se promulgó el 10 de octubre de 2018 y entró en vigor el 17 de enero de 2019. En ella se hacía frente a múltiples y homogéneas cuestiones, como la protección de datos personales y los delitos relacionados con los sistemas de información y los datos. En la Ley se revisaban, asimismo, algunas de las disposiciones del Código Penal relativas a la ciberdelincuencia. Además, se trataban cuestiones relacionadas con las pruebas electrónicas y se obligaba a los proveedores de servicios de Internet a almacenar los ficheros de registro de sus clientes durante un período de tres años.

182. En relación con el Ministerio de Justicia, el Líbano comunicó también que 20 magistrados habían recibido capacitación, con el apoyo del Consejo de Europa y la Unión Europea dentro del proyecto CyberSouth, a fin de ocuparse de las pruebas electrónicas. En el momento en que se presentó la respuesta nacional, se estaban preparando decretos legislativos del Ministerio de Justicia a fin de aplicar la Ley Núm. 81/2018.

183. El Líbano se refirió a algunos de los problemas con que había tropezado el Ministerio de Justicia en particular y el Estado en general:

a) La falta de emisión de los decretos necesarios para activar la Ley Núm. 81/2018;

b) La ambigüedad o insuficiencia de algunas disposiciones jurídicas que figuraban en la Ley Núm. 81/2018, especialmente en lo referente a la protección de datos personales y designación de una jurisdicción especializada para agilizar las cuestiones urgentes sin prever la creación de un órgano encargado de verificar que quienes practiquen el comercio electrónico faciliten los datos obligatorios (artículo 31), o con respecto a la protección frente a los anuncios promocionales (artículo 32);

c) La falta de conocimientos técnicos de todos los jueces que hacían frente a los delitos o pruebas electrónicos, así como la necesidad de desarrollar las capacidades de los jueces y los servicios de seguridad y brindarles la capacitación y el equipo necesarios para que pudieran estar a la altura de las competencias y la capacidad técnica de los delincuentes;

d) La falta de digitalización de los tribunales y su vinculación con todos los ministerios e instituciones que se ocupaban de ellos;

e) La necesidad de adoptar estrategias y políticas nacionales de ciberseguridad en el plano nacional y de establecer instituciones nacionales para aplicar esas políticas y estrategias;

f) La dificultad para hacer frente a los procedimientos del Reglamento General de Protección de Datos de la Unión Europea, que impedía a los miembros de la policía judicial acceder directamente a las direcciones IP, que antes se podían consultar;

g) Las deficiencias de los sistemas normalizados utilizados por los proveedores de servicios, como el sistema de traducción de direcciones de red (NAT) para las direcciones IP, que utilizaba el Ministerio de Comunicaciones;

h) La capacidad de los delincuentes para ocultar su verdadera identidad utilizando programas informáticos especiales (VPN, Tor, etc.), la dificultad de conocer sus ubicaciones reales y el uso de técnicas de cifrado por parte de los delincuentes para ocultar las operaciones. Todo ello impedía que los servicios de seguridad competentes desencriptaran y descubrieran la información y los datos de los delincuentes y los que habían utilizado con respecto a los delitos que hubieran cometido o tuvieran previsto cometer;

i) Los numerosos dispositivos conectados directamente a la tecnología de la información y a Internet, donde casi todos los dispositivos (refrigerador, automóvil, etc.) podían conectarse a la red mediante la Internet de las cosas sin tener en cuenta los sistemas de protección necesarios antes de comercializar esos dispositivos;

j) La falta de un plan estratégico para la transformación digital en el Líbano y de un plan ejecutivo para ello;

k) La falta de aprobación de políticas universalmente reconocidas y normas en materia de seguridad de la información en diversos departamentos e instituciones públicas;

l) La falta de difusión de una cultura de concienciación entre los miembros de la sociedad respecto de la ciberseguridad y la manera de proteger la información y los datos personales, y respecto de los riesgos de piratería informática y robo y la manera de adoptar mejores prácticas y proteger esa información y esos datos;

m) El fenómeno de la red oscura, que permitía a los delincuentes vender y comprar ilícitamente bienes y sustancias y practicar en secreto actividades delictivas, en especial el comercio de drogas, la venta de armas y el intercambio de pornografía infantil, programas maliciosos y datos personales de particulares;

n) El fenómeno de las monedas virtuales y digitales, que permitían que particulares y grupos terroristas compraran y vendieran sustancias ilícitas de manera

confidencial, sin posibilidad de rastrear las fuentes de esos fondos ni las entidades a las que se habían transferido;

o) La ausencia de un marco de cooperación internacional (convención, tratado) para el intercambio de información entre Estados con respecto a las pruebas digitales y la lucha contra la ciberdelincuencia;

p) La necesidad de un intercambio de información y de esfuerzos conjuntos entre los distintos organismos de seguridad y las instituciones de los sectores público y privado;

q) La lenta comunicación con los proveedores de servicios locales e internacionales;

r) El hecho de que no todos los delitos cibernéticos se denunciaran, especialmente los que causaban cierta vergüenza, como los relacionados con el acoso sexual y la extorsión;

s) El uso de técnicas complejas por parte de delincuentes, como los "ataques distribuidos", mediante el lanzamiento de ataques a partir de diversos servidores repartidos por el mundo, o mediante el uso de dispositivos "inteligentes" previamente pirateados como plataforma para llevar a cabo ataques contra otros objetivos.

Liechtenstein

184. Liechtenstein observó que la ciberdelincuencia iba en aumento y que la comunidad internacional se enfrentaba a una gran variedad de desafíos, en particular en los ámbitos de la investigación y persecución de esa actividad delictiva. Para Liechtenstein, actualmente los mayores desafíos eran el *phishing*, el "fraude de suplantación del Director General", la sustracción de cuentas de correo electrónico y la interceptación ilegal de datos. Estos desafíos exigían la adopción firme de medidas ejecutivas y legislativas a nivel nacional y una mejor cooperación a nivel internacional. Sin embargo, a Liechtenstein le preocupaba la tendencia a regular el ciberespacio y a penalizar, investigar y enjuiciar la ciberdelincuencia vulnerando los derechos humanos y las libertades fundamentales, especialmente el derecho a la privacidad. Liechtenstein señaló que los Estados debían observar en todo momento sus obligaciones con arreglo al derecho internacional, en particular el derecho de los derechos humanos, incluso al regular el ciberespacio y al penalizar, investigar y perseguir la ciberdelincuencia.

185. Liechtenstein informó de que su legislación nacional relativa a los delitos cibernéticos se basaba en el Convenio sobre la Ciberdelincuencia, del Consejo de Europa. Durante las últimas revisiones importantes de su Código Penal, en 2009 y 2011, se había utilizado esa Convención como marco principal de referencia internacional para la introducción de nuevas disposiciones relacionadas con Internet. El país había ratificado el Convenio en 2016, y este se seguiría utilizando como marco para las modificaciones legislativas futuras.

186. Liechtenstein expresó su apoyo al fortalecimiento del derecho internacional al objeto de regular las actividades en el ciberespacio, sobre la base de los principios de transparencia, inclusividad y cooperación y en plena conformidad con las normas vigentes de derechos humanos. El Convenio del Consejo de Europa sobre la Ciberdelincuencia había sido ratificado por Estados de todas las regiones y facilitaba enormemente la cooperación entre los Estados, armonizando la legislación, creando procedimientos y definiendo los puntos de contacto. Liechtenstein expresó su apoyo al aumento de la cooperación internacional basada en ese Convenio y se opuso a la elaboración de normativas paralelas o divergentes en el ámbito de la ciberdelincuencia, posición que había expresado junto con otras preocupaciones en su voto en contra de la resolución 73/187 de la Asamblea General.

Malasia

187. Malasia señaló que la ciberdelincuencia se había complicado debido a la evolución de tecnologías como la Internet de las cosas, la computación en la nube y la inteligencia artificial, y de servicios como el *onion router* o sistema de encaminamiento cebolla y la red oscura. Estas tecnologías eran un arma de doble filo, ya que aportaban ventajas a los Estados y a los Gobiernos, pero también a los autores de ciertos delitos. Como resultado de ello, los Gobiernos se enfrentaban a más desafíos en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

188. Malasia señaló que el entorno cibernético daba ventaja a los delincuentes debido a los elementos del seudonimato y el anonimato y planteaba desafíos a los organismos encargados de hacer cumplir la ley para detectar los delitos y vincularlos a una persona concreta. El uso generalizado del cifrado, que aportaba enormes ventajas en cuanto a asegurar la confidencialidad y la integridad, también planteaba desafíos a los organismos encargados de hacer cumplir la ley en lo que respectaba a recopilar pruebas sobre delitos cibernéticos. Los delincuentes se valían asimismo de la tecnología para realizar sus actividades delictivas. Además, había muchas aplicaciones y herramientas disponibles en Internet, especialmente las herramientas antiforenses, que se descargaban con facilidad y se podían utilizar indebidamente con fines delictivos.

189. Además, Malasia señaló que, por ejemplo, la llegada de la computación en la nube ofrecía a los delincuentes la posibilidad de almacenar información en entornos basados en la nube. La propia naturaleza de la computación en la nube planteaba desafíos nuevos a los organismos encargados de hacer cumplir la ley para descubrir y obtener pruebas digitales. El descubrimiento y la obtención de pruebas digitales desde plataformas remotas en la nube controladas por el proveedor diferían considerablemente del descubrimiento *in situ* o a nivel local. Por lo tanto, para obtener datos desde entornos basados en la nube era necesario recurrir a herramientas, técnicas y enfoques diversos.

190. Según Malasia, era necesario dar respuesta a los desafíos que enfrentaba el personal encargado de manejar las pruebas digitales y los relacionados con el mantenimiento de la cadena de custodia, y garantizar procesos completos y una infraestructura adecuada para mejorar el nivel de admisibilidad de las pruebas en los tribunales. La competencia técnica de las personas encargadas de manejar las pruebas digitales era fundamental para no exponer ni contaminar las pruebas. Por ejemplo, los organismos encargados de hacer cumplir la ley y los fiscales tenían dificultades no solo para mantener a los expertos existentes, sino también para adquirir nuevos recursos con los que efectuar las investigaciones de delitos cibernéticos. Además, era necesario mejorar las aptitudes y las competencias de los jueces y los fiscales, y aumentar sus conocimientos sobre los aspectos básicos de las tecnologías de la información y las comunicaciones y la ciberseguridad, y en particular sobre la terminología relacionada con los sistemas informáticos y de redes. Para ello, los jueces y los fiscales deberían recibir capacitación específica sobre ciberseguridad, ciberdelincuencia y tecnología de Internet.

191. En opinión de Malasia, las pruebas electrónicas eran muy volátiles y se podían modificar o eliminar fácilmente. Por lo tanto, el tiempo era esencial para la recopilación de pruebas. Malasia informó asimismo de que otro problema al que se enfrentaban las autoridades nacionales era la falta de recursos humanos de los organismos encargados de hacer cumplir la ley. Algunos organismos encargados de hacer cumplir la ley ni siquiera contaban con un equipo dedicado específicamente a las investigaciones de ciberdelincuencia. Las pruebas electrónicas solían estar en infraestructuras pertenecientes al sector privado, especialmente empresas de telecomunicaciones y proveedores de servicios de Internet, cuyas capacidades para retener y preservar las pruebas digitales diferían.

192. Como subrayó Malasia, en las investigaciones de ciberdelincuencia los organismos encargados de hacer cumplir la ley tenían que obtener las pruebas digitales transfronterizas por medio de un canal oficial, la asistencia judicial recíproca, para que

las pruebas fueran admisibles ante los tribunales. La recepción de las respuestas por ese medio podía llevar mucho tiempo, lo que podía prolongar los procedimientos judiciales. Además, las solicitudes de pruebas a otros países seguían estando sujetas a la doble incriminación.

193. Malasia también se refirió a otro problema al que se había enfrentado el Gobierno en la lucha contra el uso indebido por los delincuentes de las tecnologías de la información y las comunicaciones, como era lograr una respuesta adecuada de la legislación frente a las técnicas actuales de alta tecnología en materia de ciberdelincuencia. Además, Malasia destacó que su legislación nacional exigía que las personas encargadas de elaborar los documentos verificaran sus fuentes o acreditaran las pruebas ante los tribunales. Sin embargo, la falta de voluntad de algunos testigos, como los proveedores de servicios a nivel mundial, para prestar declaración ante los tribunales en relación con la autenticidad de un documento o fuente de información, había dado lugar a que no se procediera a la persecución.

Mongolia

194. Mongolia subrayó que, en el último decenio, el uso de Internet había aumentado rápidamente debido a las mejoras de la calidad, la velocidad y la cobertura. Por consiguiente, el número de delitos e infracciones relacionados con Internet había ido creciendo día a día. Las personas y las entidades mercantiles sufrían con frecuencia los ataques de grupos delictivos extranjeros a través de plataformas de Internet.

195. Mongolia se refirió a tres elementos fundamentales de la lucha contra la ciberdelincuencia, a saber: el seguimiento por Internet y el rastreo digital; el análisis, y la cooperación internacional. Era necesario aumentar la capacidad de lucha contra la ciberdelincuencia y cumplir las normas internacionales en la lucha contra esos delitos.

196. Mongolia declaró que se debía prestar atención especial a la ciberdelincuencia, que abarcaba diversos ciberataques, los sistemas piramidales, el *phishing*, el tráfico en línea, las amenazas en línea, las tramas de tarjetas, el fraude en línea, la pornografía infantil y los delitos contra la propiedad intelectual cometidos en Internet.

197. Como informó Mongolia, la estructura y la organización de las dependencias especializadas en ciberdelincuencia de otros Estados se dividían en los tres grupos siguientes: a) lucha contra la ciberdelincuencia cuyos objetivos eran las computadoras, las redes y los sistemas; b) lucha contra la ciberdelincuencia mediante ordenadores, redes y sistemas; y c) seguimiento, fortalecimiento e investigación de las huellas digitales. Sin embargo, a nivel nacional, el país carecía de recursos humanos para luchar contra la ciberdelincuencia, debido a la reticencia a crear capacidad y recursos humanos en ese ámbito. Por ejemplo, la Federación de Rusia tenía un centro dedicado a la seguridad en la red, cuyo objetivo era preparar a la fuerza de trabajo futura para luchar contra la ciberdelincuencia. En la actualidad, Mongolia no contaba con ninguna institución dedicada a preparar a la fuerza de trabajo futura para ello. Por lo tanto, subrayó la necesidad de que, en lo sucesivo, se dotara a la fuerza de trabajo futura de preparación y creación de capacidad para luchar contra esos delitos con la ayuda y la cooperación de los países que lideraban la lucha contra la ciberdelincuencia y, además, se capacitara y se preparara periódicamente al personal actual a fin de que tuviera la capacidad suficiente para ello.

198. Mongolia afirmó además que las direcciones IP desempeñaban un papel decisivo en la investigación de la ciberdelincuencia y las violaciones cibernéticas. No obstante, por razones financieras, tecnológicas y de programas informáticos, los proveedores de servicios de Internet en Mongolia proporcionaban una dirección IP a varios usuarios, lo que dificultaba especificar la hora y la fecha exactas del acto. En consecuencia, era bastante difícil rastrear a las personas que cometían ciberdelitos o violaciones cibernéticas. Para obtener la licencia correspondiente de la Comisión de Regulación de las Comunicaciones, los proveedores de servicios de Internet debían tener la capacidad tecnológica necesaria para garantizar que una dirección IP la compartieran como máximo 20 personas. Sin embargo, Mongolia consideró que la aplicación de ese

reglamento era inadecuada e ineficaz. Todo ello hacía que fuera casi imposible investigar con celeridad la ciberdelincuencia sin resolver el problema de la dirección IP.

199. Además, Mongolia recalcó que era necesario aclarar algunos de los términos empleados en el Código Penal. Eso sucedía por ejemplo con términos que figuraban en el artículo 26 del Código Penal de Mongolia, como “dispositivos electrónicos”, “redes protegidas” y “ataques ilegales”; su utilización en la práctica resultaba difícil, ya que no se aclaraban ni se interpretaban en otras leyes o instrumentos legislativos. Las normas y los reglamentos de otros Estados en relación con la ciberdelincuencia eran muy exhaustivos. Los elementos de esos delitos que figuraban en el Código Penal eran claros; por lo tanto, no había lugar para la confusión o la mala interpretación de los artículos en cuestión.

200. Los ciudadanos de Mongolia utilizaban principalmente plataformas sociales basadas en Internet como Facebook, Twitter, Instagram y Yahoo!, constituidas todas ellas con arreglo a la legislación y los reglamentos de Estados distintos. Por consiguiente, las autoridades nacionales no podían obtener los documentos necesarios para investigar delitos cibernéticos de entidades constituidas en el extranjero. Existía un documento de cooperación policial entre Mongolia y los Estados Unidos de América en relación con las solicitudes de entrega de documentos. No obstante, según la legislación de los Estados Unidos de América, para obtener los documentos correspondientes se necesitaba una orden judicial a tal efecto, lo que hacía que la cooperación fuera inviable.

201. En opinión de Mongolia, era necesario adoptar un programa nacional de lucha contra la ciberdelincuencia. Eso permitiría emprender medidas de política contra la ciberdelincuencia de forma escalonada y sostenible. Mongolia podría mejorar la situación actual de los reglamentos relativos a la ciberdelincuencia y crear una dependencia especializada para luchar contra ese delito.

202. En la era actual, en que la tecnología de la información evolucionaba rápidamente, era fundamental mejorar la ciberseguridad nacional y luchar contra la ciberdelincuencia. Mongolia ocupaba el puesto 84 en el Índice Mundial de Ciberseguridad de la UIT (2018). A medida que la tecnología de la información iba evolucionando, la ciberdelincuencia se volvía más compleja e incluía nuevos tipos de delitos. Era imposible eliminar la ciberdelincuencia que se cometía en Internet. No obstante, aplicando la legislación y los reglamentos pertinentes, Mongolia estaba capacitada para dar respuesta a la situación, adoptando medidas tanto de prevención como de represión.

203. Además, Mongolia declaró que las principales razones por las que algunas personas se convertían en víctimas de la ciberdelincuencia eran que el público no era consciente de los peligros y que se carecía de noticias, advertencias y conocimientos adecuados al respecto. Por lo tanto, Mongolia subrayó la necesidad de crear capacidad y sensibilizar a la opinión pública sobre los posibles peligros de la ciberdelincuencia en Internet. Era importante hacer cumplir estrictamente los requisitos técnicos, supervisar la aplicación de los reglamentos pertinentes, resolver los problemas de corto plazo relativos a las direcciones IP y otras dificultades, y aumentar la responsabilidad que tenían los proveedores de servicios de Internet a fin de prevenir, reprimir y detectar la ciberdelincuencia y luchar contra ella.

204. Mongolia señaló que de la situación actual se desprendía claramente que los organismos encargados de hacer cumplir la ley debían estar bien preparados para prevenir y combatir esos delitos. Por lo tanto, para luchar contra la ciberdelincuencia era esencial capacitar e instruir al personal y aumentar la capacidad de esos organismos de todas las formas posibles. También era necesario crear un laboratorio responsable de la detección, el fortalecimiento, la investigación y el análisis de las huellas digitales y aumentar el número de dependencias de lucha contra la ciberdelincuencia.

205. Mongolia consideraba que era necesario crear un instrumento jurídico internacional para luchar contra los delitos relacionados con la tecnología de la información y las comunicaciones.

Marruecos

206. Marruecos señaló que el mundo contemporáneo estaba experimentando una revolución de las tecnologías de la información y las comunicaciones, especialmente de los programas de procesamiento de la información y los ordenadores de gama alta desarrollados por grandes empresas. Este proceso se había visto afectado por la globalización y la transferencia fácil de información, que habían acortado las distancias entre los sistemas legales y judiciales. Estos elementos de la globalización habían dado lugar a una globalización de los delitos y de los métodos para cometerlos. A pesar de sus ventajas, la tecnología de la información se había acompañado de una serie de consecuencias negativas graves debido a su uso indebido y a las desviaciones respecto de los fines previstos, principalmente por medio de ataques contra los valores e intereses fundamentales de las personas, las instituciones y los Estados. Habían surgido una serie de delitos cometidos mediante la utilización de Internet y los medios electrónicos, lo que, a su vez, facilitaba perpetrarlos y eludir la administración de justicia (tanto en lo que respectaba a la identificación como a la localización de los autores).

207. Según las investigaciones realizadas por los servicios descentralizados de policía judicial a este respecto, Marruecos informó de que los desafíos que se planteaban en la lucha contra la ciberdelincuencia estaban generalmente relacionados con los aspectos siguientes:

a) El anonimato: la utilización de servidores intermediarios y de la red oscura;

b) La transnacionalidad: el almacenamiento de pruebas en servidores situados fuera del territorio nacional;

c) El uso frecuente del cifrado de datos;

d) El uso delictivo de las criptomonedas;

e) La evolución constante de las modalidades de funcionamiento utilizadas;

f) Las dificultades de acceso a los datos sobre el movimiento de los usuarios de determinadas aplicaciones o sitios alojados en el extranjero;

g) La planificación de la capacitación continua sobre lucha contra la ciberdelincuencia para el personal encargado de efectuar las investigaciones y manejar las pruebas digitales sobre la materia, a fin de mantenerlo al día de los avances exponenciales de la tecnología;

h) La adquisición de equipos y programas informáticos especializados adecuados y eficientes para llevar a cabo las investigaciones relacionadas con la ciberdelincuencia;

i) El hecho de que los usuarios de las tecnologías de la información y las comunicaciones deberían participar en un programa de sensibilización sobre los riesgos de incumplir las medidas de protección;

j) La activación de las estructuras de protección y las respuestas de la Comunidad de Estados Independientes ante las amenazas relacionadas con Internet;

k) La cooperación y coordinación interestatales para aclarar cuestiones jurídicas y aplicar la legislación pertinente, así como en relación con los mecanismos de investigación y la realización eficaz de investigaciones con pruebas digitales.

208. Marruecos recordó que la comunidad internacional había respondido a la ciberdelincuencia mediante la elaboración de instrumentos normativos y la aprobación de convenciones sobre la materia, y que se habían celebrado muchas conferencias. Debido a su ubicación estratégica, Marruecos también había tenido que promulgar legislación para hacer frente al fenómeno de la informática y establecer alianzas, especialmente con la Unión Europea, que habían sido muy útiles.

209. El legislador marroquí había promulgado una legislación penal adaptada a las especificidades de la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, de conformidad con los principios generales de la

justicia penal. Entre esa legislación se encontraba la Ley núm. 03.07, relativa al control de los sistemas automatizados de procesamiento de datos, aprobada en 2003 como parte del Código Penal (artículos 3/607 a 11/607). Esa ley era el marco básico de lucha contra la ciberdelincuencia en Marruecos y sus disposiciones se derivaban de las convenciones internacionales, en particular el Convenio sobre la Ciberdelincuencia del Consejo de Europa y su Protocolo Adicional, mediante el Real Decreto núm. 1.14.85, promulgado el 12 de mayo de 2014, por el que se aplicaba la Ley núm. 136.12, por la que se aprobaba el Convenio sobre la Ciberdelincuencia. Asimismo, se inspiraba en el proyecto de ley sobre directrices para combatir los delitos relacionados con la tecnología de la información.

210. Marruecos también aprobó la Convención Árabe sobre la Lucha contra los Delitos Informáticos, firmada en El Cairo el 21 de diciembre de 2010, en virtud del Decreto núm. 46.13.1, de 13 de marzo de 2013, por el que se aplicaba la Ley núm. 12.17, publicada en el Boletín Oficial núm. 6140 el 4 de abril de 2013.

211. El artículo 3 de la Ley núm. 108.13, sobre justicia militar, establecía ciertos requisitos relativos a los delitos que eran de la competencia del tribunal militar, lo que permitía a ese tribunal juzgar también la ciberdelincuencia.

212. La legislación preventiva destinada a proteger los datos personales o el intercambio electrónico de datos, como el Real Decreto núm. 1.07.129, de 30 de noviembre de 2007, por el que se aplicaba la Ley núm. 53.05 sobre el intercambio electrónico de datos jurídicos, y el Real Decreto núm. 1.09.15, de 18 de febrero de 2009, núm. 09.08, sobre la protección de datos personales, hacían de Marruecos un destino para los inversores en el ámbito de la tecnología de la información y la economía digital.

213. Por medio de la Ley núm. 96-24 sobre correo y comunicaciones, promulgada por el Real Decreto núm. 1.97.162 el 1 de agosto de 1997, modificada y complementada, y el Decreto núm. 444-08-2, de 21 de mayo de 2009, se estableció un consejo nacional de tecnologías de los medios de comunicación y economía digital, encargado de coordinar las políticas nacionales y evaluar su aplicación.

214. Igualmente, existía un proyecto de ley sobre la delincuencia organizada en materia de información con arreglo a los artículos 187, 448/1 y 448/2, que proporcionaba muchas herramientas para dar respuesta a ese delito.

215. A nivel institucional, se había establecido un equipo de tareas de la policía judicial para combatir la ciberdelincuencia. En el aparato de seguridad nacional marroquí se habían creado dos dependencias de lucha contra el terrorismo para combatir los delitos relacionados con los sistemas de información, tanto a nivel de investigación como de seguimiento de los delincuentes a través de Internet. El Ministerio de Defensa Nacional había creado la Dirección de Ciberdelincuencia para hacer frente a ese tipo de delitos, rastrear sus efectos y combatirlos en coordinación con diversos departamentos de seguridad nacionales e internacionales.

216. A pesar de esos esfuerzos, Marruecos subrayó que la lucha contra esos delitos seguía planteando muchos desafíos. Era difícil que la legislación respondiera al rápido desarrollo de la ciberdelincuencia y, por ejemplo, a la ausencia de un marco jurídico para los delitos cometidos por medio de las redes sociales. La mayoría de las disposiciones legales actuales se referían a los usuarios de los medios sociales y no incluían ningún requisito que estableciera la responsabilidad de los proveedores de servicios de red y los obligara a eliminar, bloquear, detener o desactivar el acceso a contenidos electrónicos ilegales. Esto se veía agravado por el hecho de que la mayoría de esos proveedores y los directivos de esas plataformas se hallaban fuera de la jurisdicción del país.

217. Marruecos destacó que la cooperación internacional en la lucha contra la ciberdelincuencia planteaba también dificultades respecto de la comunicación con los proveedores de servicios de telecomunicaciones de otros países, que exigía la adopción de un instrumento internacional que permitiera la cooperación directa con esos proveedores para garantizar la conectividad transfronteriza de los datos.

218. Por otra parte, Marruecos resaltó asimismo que la lucha contra la ciberdelincuencia planteaba un desafío mayor en cuanto al fortalecimiento de la capacidad de los organismos encargados de hacer cumplir la ley. La evolución amplia y continua de las técnicas de ciberdelincuencia, como los delitos relacionados con Internet, los ciberataques, los ataques de *phishing*, el *phishing* electrónico, el acceso a Internet, las monedas virtuales, la computación en la nube y la criptografía, exigía que los órganos de investigación modificaran sus estrategias en la búsqueda e investigación de inferencias delictivas y proporcionaran un directorio electrónico aceptable y fidedigno a los ojos de la judicatura.

Myanmar

219. Myanmar señaló que la lucha contra la ciberdelincuencia era vital para proteger la ciberseguridad nacional y la infraestructura nacional de información. Era urgente elaborar una legislación nacional adecuada, compatible con las normas internacionales, para lograr la máxima eficacia en la lucha contra la ciberdelincuencia. Los organismos encargados de hacer cumplir la ley debían contar con los instrumentos jurídicos, las herramientas técnicas y la infraestructura y los mandatos apropiados que eran necesarios para llevar a cabo investigaciones eficaces y enjuiciamientos satisfactorios.

220. Además, Myanmar subrayó que la búsqueda de estrategias y soluciones ante la amenaza de la ciberdelincuencia era un desafío importante para los países en desarrollo. En cuanto a las disparidades territoriales, los responsables de sitios web con contenidos ilegales trasladaban sus actividades a países en los que no se penalizaban dichos contenidos con el fin de evitar las investigaciones penales. Esos traslados a países extranjeros eran uno de los problemas que enfrentaban los organismos encargados de hacer cumplir la ley, ya que los servidores se encontraban fuera del territorio de su país. Los delincuentes aprovechaban plenamente esas disparidades territoriales y no difundían, distribuían, compartían ni almacenaban contenidos ilegales ni imágenes ofensivas en los discos duros locales, sino en servidores externos a los que podían acceder a través de Internet. En consecuencia, la cooperación internacional era fundamental para descubrir a los delincuentes y superar las dificultades derivadas de las disparidades territoriales. Al adoptar políticas nacionales de ciberseguridad y crear los marcos jurídicos apropiados se debían tener en cuenta la compatibilidad con la legislación nacional existente y la adecuación a las normas internacionales.

221. Myanmar informó de que el Estado se había encontrado con las dificultades siguientes al elaborar la política de ciberseguridad y los instrumentos jurídicos subsiguientes:

a) Era necesario adoptar un marco integral de política nacional y una legislación adecuada de lucha contra la ciberdelincuencia que fueran compatibles con las prácticas y los procedimientos internacionales. El Estado debía adaptar sus estrategias de ciberseguridad y de lucha contra la ciberdelincuencia a las normas internacionales;

b) Era fundamental realizar un análisis exhaustivo de la legislación nacional actual para detectar posibles lagunas y superposiciones entre la ciberlegislación y otras leyes del derecho positivo. La revisión detallada de la legislación pertinente llevaba mucho tiempo y, asimismo, requería aplicar estándares profesionales altos y tener en cuenta conceptos basados en prácticas internacionales y en el intercambio de opiniones;

c) Era necesario establecer un organismo encargado de hacer cumplir la ley para garantizar que la seguridad nacional y el estado de derecho se ajustaran a los derechos fundamentales de los ciudadanos. Al mismo tiempo, había que crear un centro de interceptación conforme a derecho para llevar a cabo la vigilancia de las comunicaciones mediante la adopción de procedimientos operativos estándar de interceptación conformes a derecho y basados en los principios y normas internacionales sobre protección de datos y salvaguardias de privacidad;

d) Se deberían establecer equipos de respuesta a los ciberincidentes y ciberataques (es decir, equipos de respuesta a emergencias informáticas, equipos de

respuesta a incidentes informáticos y equipos de respuesta a incidentes de seguridad informática) que estuvieran bien cualificados para gestionar las cibercrisis y evaluar las amenazas y las vulnerabilidades. Estos equipos debían de difundir información sobre seguridad y ofrecer asesoramiento al respecto en lo relativo a ciberincidentes, riesgos cibernéticos, ciberataques y posibles riesgos de esos ciberataques para el público, y prestar apoyo a los organismos encargados de hacer cumplir la ley mediante la asistencia técnica necesaria para que pudieran llevar a cabo investigaciones eficaces;

e) El Estado debería destinar fondos a la adopción de medidas técnicas de protección para crear una Internet segura y fiable y para garantizar la seguridad de Internet y las salvaguardias de la red, incluso mediante el suministro de la infraestructura, las instalaciones y el equipo necesarios para implementar esas medidas de protección y actividades de seguridad;

f) Si bien se debían adaptar los marcos legislativos nacionales relativos a las redes informáticas con el fin de regular las investigaciones penales, era importante tener en cuenta las salvaguardias de los derechos humanos al utilizar los datos personales;

g) Se necesitaban normas claras y precisas sobre protección de datos y salvaguardias de privacidad para los sectores privados que intervenían en la recopilación, el almacenamiento o el intercambio de los datos de los usuarios;

h) Los usuarios de Internet deberían recibir información precisa sobre la ciberseguridad, la naturaleza y los tipos de ciberdelincuencia y la realidad complicada y compleja de los ciberataques. Además, se deberían financiar campañas de sensibilización y cursos de capacitación para los usuarios y se debería mejorar la alfabetización digital en los casos en que se adaptaran las tecnologías de la información y las comunicaciones interconectadas a nivel mundial a los usuarios nacionales.

222. En Myanmar, los casos de fraude y difamación en línea eran frecuentes. Lo más habitual en ese sentido era la utilización de la información y las comunicaciones en línea para incitar disturbios raciales y religiosos y para amenazar a trabajadores y organizaciones gubernamentales. Myanmar se enfrentaba principalmente al uso de los medios sociales en actos de terrorismo, con fines propagandísticos y para agresiones personales. En las investigaciones penales, las autoridades no obtenían información específica ni cooperación de los proveedores de servicios de Internet.

223. Además, Myanmar informó de que, en los casos en que era necesario solicitar información sobre los abonados a las empresas de medios sociales radicadas en el extranjero, las empresas denegaban las solicitudes aduciendo que no se ajustaban a los procedimientos estándares. En consecuencia, había dificultades para efectuar las investigaciones.

224. Myanmar también reseñó que las investigaciones tropezaban con numerosas dificultades debido a los escasos recursos con que contaban los técnicos, el desconocimiento de los usuarios en línea y el escaso efecto jurídico vinculante de las leyes y los procedimientos. A medida que la tecnología evolucionaba y permitía acceder a la banca móvil por medio de teléfonos móviles, los ciberataques se iban dirigiendo a los usuarios de teléfonos móviles.

225. Myanmar opinó que los mecanismos jurídicos existentes eran insuficientes para combatir los delitos cometidos mediante el uso de las tecnologías de la información y las comunicaciones. Informó de que se estaba redactando legislación en materia de derecho informático, así como políticas conexas sobre gobierno electrónico, comercio electrónico y ciberseguridad, y que el proyecto se estaba ejecutando bajo la dirección del Ministerio de Transporte y Telecomunicaciones con el asesoramiento de una empresa consultora externa.

226. Myanmar señaló que el problema se podía solucionar mediante la elaboración y aprobación de una convención de las Naciones Unidas, ya que era necesaria la cooperación internacional.

227. Myanmar expresó su acuerdo con que, para dar respuesta a la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, era necesario

un debate permanente y abierto en el que participaran todos los Estados interesados. Dicho debate se podría celebrar en el marco de un grupo de trabajo de composición abierta de las Naciones Unidas encargado de elaborar los documentos correspondientes y de adoptar decisiones por mayoría de votos. Asimismo, Myanmar valoró y se mostró de acuerdo con que el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético se centrara principalmente en las cuestiones relativas a la lucha contra los delitos de información.

Países Bajos

228. Los Países Bajos señalaron que era una responsabilidad compartida de la comunidad internacional de policía y justicia impedir que Internet se convirtiera en un lugar seguro para los delincuentes, y que no se debía permitir que la delincuencia fuera rentable. Para luchar contra la ciberdelincuencia era esencial contar con instrumentos jurídicos eficaces que respetaran los derechos humanos fundamentales. Se podían distinguir instrumentos de ámbitos diversos, a saber: nacionales, regionales e internacionales. En primer lugar, muchos países habían fortalecido su capacidad nacional para combatir la ciberdelincuencia. No obstante, existían disparidades internacionales en cuanto a derecho penal, conocimientos especializados y equipos, lo que dificultaba dar respuesta y hacer frente a un fenómeno de tal carácter transfronterizo. Este fenómeno solo se podía afrontar intensificando las actividades de creación de capacidad dentro de los Estados y entre ellos. Una red internacional amplia de organismos encargados de hacer cumplir la ley capacitados permitiría asestar un duro golpe a la ciberdelincuencia organizada. Un segundo tipo de instrumentos eran los regionales. Se denominaban así porque los países que no eran de la región en cuestión no tenían acceso a ellos. Ejemplos de ese tipo de iniciativas eran la iniciativa sobre las pruebas electrónicas de la Unión Europea y los marcos de la Organización de Cooperación de Shanghái, las organizaciones intergubernamentales africanas y la Liga de los Estados Árabes. En tercer lugar, existían instrumentos internacionales abiertos a los países de todo el mundo. Ejemplos de ese tipo de instrumentos eran el Convenio sobre la Ciberdelincuencia del Consejo de Europa, que contaba con 63 partes (cifra que seguía aumentando), además de otros 70 Estados que tenían el Convenio como modelo de legislación, y la Convención contra la Delincuencia Organizada y sus Protocolos. Al ser uno de los primeros Estados en firmar y ratificar el Convenio del Consejo de Europa, los Países Bajos habían experimentado los beneficios del Convenio en cuanto a la obtención de resultados en las investigaciones penales, adaptando la legislación nacional al aumento de las posibilidades de cooperación con otros Estados partes. Los Países Bajos también subrayaron los beneficios del marco de la Convención contra la Delincuencia Organizada.

229. Los Países Bajos declararon que las necesidades prácticas más pertinentes y urgentes para la aplicación de la ley en el ciberespacio eran, en primer lugar, el acceso transfronterizo a las pruebas electrónicas y, en segundo lugar, la cooperación internacional en las investigaciones penales. La cooperación bilateral y la asistencia judicial recíproca eran insuficientes en los casos de delitos transfronterizos que evolucionaban con rapidez. Hoy en día, el acceso a las pruebas electrónicas era necesario para todos los tipos de delitos, dado el uso de las tecnologías de la información y las comunicaciones, especialmente de las muchas herramientas novedosas como los medios sociales y la mensajería basada en la web, que habían dado lugar a un aumento sin precedentes de los datos digitales. La cooperación internacional solo se podía mejorar si los organismos encargados de hacer cumplir la ley tenían la capacidad y la aptitud necesarias para participar, por ejemplo, en investigaciones conjuntas. Ya se estaban desarrollando y debatiendo enfoques innovadores para el acceso transfronterizo a las pruebas electrónicas, como las órdenes de presentación de documentos o los registros ampliados de las redes. Las negociaciones en curso sobre un protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa ponían de manifiesto la voluntad compartida por muchos Estados de adaptar el marco existente para conseguir efectivamente una mejora de la justicia penal en el ciberespacio.

230. Los Países Bajos afirmaron que uno de los grandes desafíos en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos era el de permitir que los instrumentos existentes alcanzaran su pleno potencial y no desviar los recursos y las fuerzas, que ya eran escasos, hacia un proceso prolongado de búsqueda de un nuevo marco supranacional. El Convenio sobre la Ciberdelincuencia del Consejo de Europa era ya un resultado tangible cuyo valor añadido se demostraba día a día. Los organismos encargados de hacer cumplir la ley y las autoridades judiciales, desde los Estados Unidos de América hasta Sri Lanka y desde el Japón hasta el Senegal, tenían acceso a las distintas posibilidades que ofrecía el Convenio, lo que brindaba resultados concretos en las investigaciones penales. Con el Protocolo Adicional al Convenio se había dado ya un paso dentro de las medidas siempre necesarias para estar al día y ofrecer soluciones de vanguardia.

231. Con el paso del tiempo se habían realizado grandes esfuerzos de creación de capacidad, pero aún quedaba mucho trabajo por hacer, y este era el segundo gran desafío. Este trabajo se podía afrontar desde una perspectiva bilateral o conjuntamente con la Oficina del Programa de la Ciberdelincuencia del Consejo de Europa y la UNODC. Cuando se trataba de las Naciones Unidas, el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético se encontraba en una posición ideal para fomentar la creación de una plataforma de intercambio de opiniones y mejores prácticas. Los Países Bajos informaron de que, durante las consultas a fondo del año anterior y del año en curso, el Grupo de Expertos había mejorado considerablemente la ejecución de su plan de trabajo para 2017. Los Países Bajos esperaban que ese proceso se tradujera en la obtención en 2021 de una visión general más actual y presente de los desafíos de la justicia penal en el ciberespacio, así como de recomendaciones orientativas para el futuro.

232. Los Países Bajos pidieron que prosiguieran las mejoras que el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético había experimentado en 2017 y expresaron su confianza absoluta en que el énfasis en la asistencia técnica facilitaría la transferencia de las mejores prácticas y el fomento de la capacidad en todo el mundo. Exhortaron a participar en las negociaciones en curso, cuyo valor había quedado demostrado, y que habían arrojado resultados. Asimismo, pidieron a los demás Estados que no pusieran en marcha nuevas iniciativas que desviaran los recursos y las fuerzas de esas negociaciones.

Nueva Zelandia

233. Nueva Zelandia señaló que el aislamiento geográfico del país lo había protegido históricamente de algunas amenazas. Pero la distancia no ofrecía ninguna protección ante la ciberdelincuencia, para la cual no existían fronteras. Entre los desafíos concretos a los que se enfrentaba Nueva Zelandia para luchar contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos figuraban los siguientes:

a) Una imagen incompleta de la ciberdelincuencia en Nueva Zelandia y en todo el mundo;

b) Dificultad para calcular los costos de la ciberdelincuencia;

c) Dificultad para detectar, investigar y enjuiciar la ciberdelincuencia;

d) Cuestiones derivadas de las responsabilidades compartidas entre el Gobierno, las organizaciones no gubernamentales, el sector privado y los particulares.

234. Nueva Zelandia informó de que, para dar respuesta a la ciberdelincuencia, centraba su atención en que la legislación se adecuara a los fines previstos y en adoptar un enfoque integrado, así como en la sensibilización y la capacitación y en la cooperación internacional. La información proporcionada a los efectos del presente informe se había obtenido del Plan Nacional de Lucha contra la Ciberdelincuencia (2015), que estaba disponible en línea.

235. No existía una imagen completa de la ciberdelincuencia. Esta se podía distinguir de la “delincuencia tradicional” por los desafíos que su naturaleza global planteaba a los organismos encargados de hacer cumplir la ley. Las personas o grupos podían actuar desde cualquier lugar en el extranjero en el que hubiera una conexión a Internet. La inmensa mayoría de los autores de ese tipo de delitos se encontraban en el extranjero y estaban muy organizados. En todo el mundo había muchos casos de ciberdelincuencia que no se denunciaban. En algunos casos, las víctimas no sabían que habían sido objeto de un delito. A otras les daba mucha vergüenza denunciar los delitos, no sabían a quién denunciarlos o no creían que los organismos encargados de hacer cumplir la ley pudieran darles una solución. Si las víctimas obtenían una reparación de un proveedor o institución financiera, no siempre denunciaban el delito. Por último, las empresas se podían mostrar reacias a revelar pérdidas o fallos por temor a un deterioro de su reputación.

236. Los costos de la ciberdelincuencia eran difíciles de calcular y sus costos indirectos, incluidos los costos de oportunidad, eran difíciles de cuantificar. Para muchas pequeñas y medianas empresas, la ciberdelincuencia podía dar lugar a una “denegación de la actividad”, es decir, no les podían robar nada, pero un ataque podía reducir su capacidad para comerciar. Las empresas y los particulares también debían afrontar costos para protegerse contra la ciberdelincuencia y para las reparaciones (en su caso). La ciberdelincuencia podía posibilitar asimismo la organización y la perpetración de delitos físicos, como el fraude, la extorsión, los disturbios y las agresiones sexuales y otras agresiones violentas. La ciberdelincuencia podía causar daños sociales derivados de la vergüenza y las molestias y, en casos más graves, daños físicos o emocionales. Si bien las pérdidas financieras ocasionadas por la ciberdelincuencia podían ser pequeñas en un caso concreto, con el tiempo los efectos sobre la confianza pública podían ser corrosivos. La ciberdelincuencia ofrecía al delincuente un gran rendimiento con un costo bajo y un riesgo razonablemente pequeño. Las pérdidas que miles de correos basura podían generar para las distintas víctimas podían ser pequeñas, pero para Nueva Zelandia en conjunto la pérdida podía ser mucho mayor.

237. Resultaba difícil detectar, investigar y enjuiciar la ciberdelincuencia. Su naturaleza mundial hacía que fuera complicado buscar a los autores y acceder a las pruebas conexas. El intercambio de información y la cooperación entre los distintos países podían ser deficientes y, aun cuando existieran relaciones de cooperación sólidas, los procesos de los tratados de asistencia judicial recíproca podían ser muy lentos y engorrosos. Los casos podían precisar un esfuerzo de investigación desproporcionado, lo que reducía la disponibilidad de recursos para hacer frente a otras exigencias. Asimismo, podría suceder que el país en el que se encontrara el autor del delito no tuviera la capacidad necesaria para llevar a cabo una investigación o preservar las pruebas.

238. Las investigaciones se complicaban aún más por la capacidad que brindaba Internet de actuar de forma casi anónima. La atribución de los ciberincidentes era muy difícil, especialmente cuando los ataques se originaban en el extranjero. Esto convertía a la ciberdelincuencia en un desafío, no solo en lo relativo a la investigación sino también para la persecución. Los delincuentes que intentaban ocultar su identidad bajo capas de cifrado podían aprovechar para ello los servidores intermediarios y los canales como el *onion router* y las redes entre pares. Esas redes se utilizaban con frecuencia para facilitar la actividad delictiva y dificultaban la labor de los organismos encargados de hacer cumplir la ley. Tanto esas redes como los sitios de la red oscura estaban ofreciendo además servicios de ciberdelincuencia, como piratas informáticos de alquiler o simples juegos de herramientas. Esa evolución reducía las barreras de acceso a la ciberdelincuencia. De esa forma, un grupo de agentes no cualificados podían tener un impacto relativamente perjudicial. En el otro extremo del espectro, a medida que proliferaban las actividades y las técnicas se volvían cada vez más sofisticadas, las fronteras entre los agentes delictivos y los agentes estatales (algunos de los cuales también podían actuar con intención delictiva) se iban difuminando. A medida que la tecnología y las estrategias de detección evolucionaban, también lo hacían los agentes, con lo que para los encuestados era difícil mantenerse al día. Los delincuentes no rehusaban la utilización de tecnología de anonimato, en particular programas como

el *onion router*, para intentar ocultar sitios que proporcionaban material de explotación infantil y tráfico de drogas.

239. La respuesta de Nueva Zelandia a la ciberdelincuencia era una respuesta compartida entre el Gobierno, las organizaciones no gubernamentales, el sector privado y los particulares. Una serie de organismos gubernamentales de Nueva Zelandia tenían responsabilidades operacionales y de política relacionadas con la ciberdelincuencia. Esas funciones habían evolucionado en gran medida de manera orgánica, más que intencionada. La ciberdelincuencia era un problema compartido y las organizaciones no gubernamentales, la sociedad civil y el sector privado tenían un papel que desempeñar tanto en la prevención como en la respuesta. Esa responsabilidad compartida podía dar lugar a desafíos. Algunos incidentes se denunciarían en varios lugares, y las víctimas podían ser remitidas de un organismo a otro en el afán de encontrar el mejor lugar para la solución. Las respuestas también podían variar dentro de cada servicio. Nueva Zelandia había avanzado en ese ámbito con la creación del equipo informático de respuesta de emergencia (CERT NZ) en 2016. El CERT NZ era un organismo que proporcionaba más claridad sobre dónde denunciar los ciberincidentes, una derivación más eficiente de los ciberincidentes a los organismos pertinentes y un asesoramiento más funcional y oportuno a los organismos, las empresas y los individuos. Muchas empresas del sector privado también ofrecían respuesta a la ciberdelincuencia como parte de sus servicios básicos al cliente. El Gobierno tenía la oportunidad de mejorar la experiencia de las víctimas de ciberdelincuencia y, al mismo tiempo, adquirir una mejor comprensión del tema y sensibilizar a la opinión pública.

Nicaragua

240. Nicaragua consideró que las regulaciones jurídicas en los instrumentos existentes por el derecho penal eran insuficientes para luchar contra los delitos cometidos con el uso de las tecnologías de la información y las comunicaciones. Muchos países habían sido víctimas de dichos delitos. Por lo tanto, Nicaragua estaba convencida de que el tema debía ser analizado por las Naciones Unidas, con la finalidad de elaborar y aprobar un convenio internacional sobre cooperación y regulación en esa esfera.

241. Asimismo, Nicaragua consideró oportuno iniciar lo más pronto posible la conformación de un grupo de trabajo de composición abierta, a fin de avanzar en el establecimiento de la regulación internacional de los delitos cometidos con el uso de las tecnologías de la información y las comunicaciones.

Noruega

242. Noruega se refirió a la información que había enviado a la UNODC el 4 de marzo de 2019 sobre las medidas e iniciativas que se habían adoptado en el país contra la ciberdelincuencia en relación con la labor del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético[8].

243. Noruega había ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa en 2005 y estaba siguiendo de cerca el proceso de elaboración del Segundo Protocolo Adicional. Dio su respaldo al Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético como proceso principal a nivel de las Naciones Unidas en relación con el tema de la ciberdelincuencia, al menos hasta 2021.

244. Noruega señaló que, a medida que se iban desarrollando las amenazas en el ámbito de la ciberdelincuencia, había que reforzar las respuestas a los desafíos, pues la falta de medidas eficaces podía suponer una amenaza para el estado de derecho. Las pruebas electrónicas eran cada vez más útiles en las causas penales. Esos datos se almacenaban a menudo en el extranjero, lo que dificultaba su localización y obtención. La cooperación a nivel nacional e internacional era fundamental. Se necesitaban marcos

[8] Disponible en https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

internacionales más eficaces, ya que los organismos encargados de hacer cumplir la ley estaban limitados por las fronteras nacionales. Al mismo tiempo, la observancia de los derechos fundamentales y un alto grado de sensibilización respecto de las salvaguardias deberían ser ejes centrales de las iniciativas encaminadas a elaborar los nuevos instrumentos internacionales.

245. Noruega confirmó que adquiriría la aptitud, las competencias y la capacidad técnica suficientes para hacer frente a tipos de delitos nuevos y en constante evolución. Señaló que un elemento fundamental de su labor nacional sería comprender mejor las amenazas que afectaban a la esfera digital. También era importante considerar los nuevos desafíos en el contexto de la delincuencia más tradicional. La ciberdelincuencia no era un tipo de delito aislado, sino un elemento transversal en muchos tipos de delitos, incluidos el terrorismo y la delincuencia organizada transnacional. La acción concertada entre los Gobiernos y el sector privado era una parte esencial de la solución.

246. Noruega destacó además que, de conformidad con la Ciberestrategia Nacional para Noruega (2017), las autoridades del país velaban por que hubiera una coordinación estrecha entre los órganos que representaban al país en los foros en que se formulaban las políticas internacionales de ciberseguridad y se desarrollaba la cooperación en materia de ciberdelincuencia y tratamiento de los ciberincidentes. Noruega apoyaría los enfoques de colaboración para buscar soluciones adecuadas dentro de la labor constante que se desarrollaba a escala internacional a fin de combatir la ciberdelincuencia, manteniendo al mismo tiempo los valores democráticos y protegiendo los derechos humanos universales.

Perú

247. El Perú informó de que, en 2016, el Banco Interamericano de Desarrollo había elaborado en coordinación con la Organización de los Estados Americanos el informe de 2016 sobre la Ciberseguridad en América Latina y el Caribe. Luego de la evaluación de 49 indicadores que abordaban ámbitos diversos (política y estrategia, cultura y sociedad, educación, marcos legales, y tecnologías), se habían consignado cuatro desafíos principales para el Perú, a saber:

a) Fortalecer las capacidades de defensa cibernética de las fuerzas armadas;

b) Fortalecer las capacidades técnicas de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) para el manejo de pruebas electrónicas;

c) Fortalecer la conciencia social de seguridad cibernética;

d) Mejorar las capacidades de los docentes de universidades y empresas de capacitación.

248. De acuerdo con el *Microsoft Security Intelligence Report* de 2017, el 16,9 % de las computadoras en el Perú estaban infectadas con programas maliciosos (*malware*) en comparación con el 7,8 % del promedio mundial. Igualmente, la infección a través de troyanos (8,13 %), programas parásitos (gusanos) (5,7 %) y virus (0,92 %) en el país estaba por encima del promedio mundial.

249. Un reciente estudio elaborado por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros del Perú había indicado que un 22,6 % de las entidades de la administración pública no tenían la capacidad para implementar su “Sistema Generalizado de Seguridad Digital”. Se señalaron los motivos siguientes:

a) No contar con los recursos económicos necesarios para su implementación;

b) El 50,9 % manifestaba no contar con personal suficiente;

c) El 22,6 % refería no contar con los conocimientos suficientes para iniciar la implementación;

d) El 16 % señalaba que no era un tema prioritario para su sector.

250. El impacto negativo de los riesgos de la seguridad de la información era alto en los activos críticos de la organización, lo que generaba costos económicos y pasivos para las entidades. En diversos casos se interrumpían o detenían los procesos principales de negocio y se producían chantajes o extorsiones con el pago de grandes sumas de dinero para la recuperación de la información.

251. En cuanto a los desafíos prioritarios, el Gobierno del Perú consideraba necesaria la creación de una fiscalía especializada en delitos informáticos, mayores capacitaciones para el personal fiscal sobre la materia, y que una institución asumiera la prevención de los delitos informáticos hacia los ciudadanos. Se había registrado un crecimiento importante en la cantidad de denuncias en delitos informáticos, especialmente en la modalidad de fraude informático. Las principales modalidades que se debían enfrentar eran las siguientes:

a) El fraude informático a través de "*carding*", por el que las organizaciones criminales utilizaban la información confidencial de las tarjetas bancarias para realizar compras por Internet en tiendas virtuales con dominios web y servidores ubicados en el extranjero. Ello dificultaba la obtención de información de manera oportuna por la regulación de las leyes en cada país que protegía la información que cada empresa debía proporcionar;

b) La suplantación de identidad a través de las redes sociales, debido a la libertad con la cual los usuarios podían crearse una cuenta y navegar de forma anónima, inclusive creando diferentes nombres que eran utilizados de forma ilícita;

c) La captación de niños por Internet con fines sexuales (*grooming*), que consistía en que las organizaciones criminales simulaban ser niños con la finalidad de inducir a sus víctimas a desnudarse a través de las cámaras de vídeo de las computadoras portátiles o de sobremesa. En otros casos, se sostenían encuentros presenciales donde se obtenía material pornográfico infantil para ser comercializado e intercambiado con otros pedófilos a nivel nacional e internacional, inclusive a través de aplicaciones como WhatsApp;

d) El chantaje y la extorsión realizados por parejas luego de haber tenido relaciones sexuales filmadas, bajo la amenaza de publicar por Internet las referidas intimidades. Ello con diferentes finalidades, como obtener un beneficio económico o retomar la relación sentimental;

e) Los ataques de piratas informáticos *(hackers)* activistas en ejecución de campañas cuyo objetivo era afectar la imagen institucional y que hacían uso de redes anónimas como el *onion router*, que permitían que sus ataques provinieran de países de Asia, imposibilitando así su identificación. Asimismo, se recibían ataques de comercialización de la información institucional, que buscaban obtener información masiva de entidades con fines delictivos. También existía la posibilidad de que los medios de comunicación realizaran ciberataques o ciberespionaje para conseguir las primicias deseadas.

Filipinas

252. Filipinas se refirió a la ciberdelincuencia como un problema social grave y señaló que el ciberespacio se consideraba una nueva dimensión (además de la tierra, el aire y el agua) que el Gobierno tenía que regular y cuya consideración exigía ampliar los mandatos de los organismos encargados de hacer cumplir la ley. Para garantizar la seguridad de la población, el Gobierno había reconocido la necesidad de dotar a los organismos encargados de hacer cumplir la ley mediante las leyes siguientes: Ley de Prevención de la Ciberdelincuencia de 2012 (Ley de la República núm. 10175), Ley de Comercio Electrónico de 2000 (Ley de la República núm. 8792), Ley Contra la Fotografía y el Voyerismo de 2009 (Ley de la República núm. 9995), Ley contra la Pornografía Infantil de 2009 (Ley de la República núm. 9725), Ley contra la Trata de Personas de 2003 (Ley de la República núm. 9208), Ley de Regulación de los

Dispositivos de Acceso de 1998 (Ley de la República núm. 8484) y Ley de Privacidad de Datos de 2012 (Ley de la República núm. 10173).

253. Filipinas se adhirió al Convenio sobre la Ciberdelincuencia del Consejo de Europa el 20 de febrero de 2018 y había atendido las solicitudes internacionales relativas a la preservación de datos, el suministro de información sobre los abonados, la recopilación de datos informáticos y comerciales y la incautación de nombres de dominio.

254. En este contexto, en la legislación nacional se consideraba que la especialización era fundamental para obtener buenos resultados en la investigación y el enjuiciamiento de los ciberdelincuentes. Conforme a la Ley de Prevención de la Ciberdelincuencia de 2012, se habían creado las siguientes autoridades especializadas para hacer frente a la ciberdelincuencia y a las cuestiones conexas:

a) Oficina de Ciberdelincuencia del Departamento de Justicia: autoridad central con arreglo a la Ley de Prevención de la Ciberdelincuencia para velar por la aplicación del Convenio sobre la Ciberdelincuencia del Consejo de Europa, incluidas las cuestiones relacionadas con la asistencia recíproca internacional y la extradición;

b) Centro de Investigación y Coordinación sobre Ciberdelincuencia: órgano interinstitucional bajo la supervisión administrativa del Departamento de Tecnología de la Información y las Comunicaciones, en virtud de la Ley de la República núm. 10844 de 2015, encargado de coordinar las políticas entre los organismos pertinentes y de formular y ejecutar el plan nacional de ciberseguridad;

c) División de Ciberdelincuencia de la Oficina Nacional de Investigación: se había reorganizado para mejorar de forma efectiva su capacidad forense digital, de ciberseguridad y de respuesta ante ciberincidentes, tal como se establecía en la Ley de Ciberdelincuencia. En el marco de esta división se habían creado tres centros regionales sobre ciberdelincuencia, se habían adquirido herramientas y programas informáticos forenses nuevos y actualizados y se había impartido la capacitación correspondiente para los examinadores digitales;

d) Grupo contra la Ciberdelincuencia de la Policía Nacional: establecido junto con nueve oficinas regionales contra la ciberdelincuencia en todo el país. Había creado cuatro cursos especializados de lucha contra la ciberdelincuencia que eran necesarios para los agentes de policía que se especializaban en ciberdelincuencia.

255. Las Fuerzas Armadas de Filipinas, encabezadas por el Jefe de Gabinete Adjunto del Servicio de Sistemas de Información, Electrónica y Comunicaciones, estaban elaborando un plan estratégico para el ciberespacio a fin de proporcionar una hoja de ruta con miras a materializar una organización plenamente apta para el ciberespacio para 2022.

256. El Consejo de Lucha contra el Blanqueo de Dinero era la dependencia de inteligencia financiera del país encargada de aplicar la Ley contra el Blanqueo de Dinero, modificada por las Leyes de la República núm. 9194, 10167 y 10365, así como la Ley de la República núm. 10168, también conocida como Ley de Prevención y Represión de la Financiación del Terrorismo de 2012.

257. En enero de 2017 el poder judicial contribuyó asimismo a las iniciativas para combatir la ciberdelincuencia mediante la designación de tribunales de ciberdelincuencia encargados de juzgar los casos previstos en la Ley de Prevención de la Ciberdelincuencia de 2012, además de su designación como tribunales comerciales.

258. Filipinas informó también de que, a nivel nacional, se habían establecido los siguientes mecanismos de cooperación interinstitucional:

a) El Subcomité de Ciberdelincuencia del Comité Nacional de Coordinación de la Aplicación de la Ley, que fortalecía la coordinación interinstitucional para combatir la ciberdelincuencia y otras actividades conexas prestando asistencia a las campañas de lucha contra la ciberdelincuencia de otros Estados, por ejemplo, facilitando el intercambio de información y la detención de personas implicadas en ese tipo de delitos;

b) El Consejo Interinstitucional contra la Trata, que promulgaba normas y reglamentos para la aplicación efectiva de la Ley de la República núm. 9208, o Ley contra la Trata de Personas de 2003, modificada por la Ley de la República núm. 10364, o Ley Ampliada contra la Trata de Personas de 2012. Estaba encabezado por el Secretario de Justicia, lo que a su vez aceleraba la coordinación de los programas y los proyectos para abordar de manera eficaz las cuestiones relacionadas con la trata de personas. El Consejo recomendaba medidas para mejorar la asistencia recíproca entre países extranjeros mediante acuerdos bilaterales o multilaterales, a fin de prevenir y reprimir la trata internacional de personas;

c) El Consejo Interinstitucional contra la Pornografía Infantil, encabezado por el Secretario de Bienestar Social y Desarrollo e integrado por otros organismos gubernamentales y organizaciones no gubernamentales pertinentes, que formulaba planes y programas amplios e integrados para prevenir y reprimir cualquier forma de pornografía infantil y para presentar denuncias contra personas, organismos, instituciones o establecimientos que contravinieran las disposiciones de la Ley contra la Pornografía Infantil de 2009 (Ley de la República núm. 9775).

259. En cuanto a las buenas prácticas en la aplicación de la ley y en la investigación, Filipinas reconoció la importancia de utilizar organismos especializados en ambas materias. Para Filipinas, la cooperación interinstitucional era fundamental para la aplicación efectiva de la ley y la investigación de los casos, bajo la dirección del Subcomité de Ciberdelincuencia del Comité Nacional de Coordinación de la Aplicación de la Ley, el Consejo Interinstitucional contra la Trata y el Consejo Interinstitucional contra la Pornografía Infantil.

260. También se señaló que otro mecanismo que utilizaban los organismos encargados de hacer cumplir la ley era INTERPOL, y que la Oficina Central Nacional de INTERPOL en Manila funcionaba como órgano principal de coordinación de la cooperación policial nacional e internacional en la lucha contra los delitos transnacionales. La cooperación estrecha con los organismos encargados de hacer cumplir la ley, otros organismos gubernamentales y los organismos extranjeros encargados de hacer cumplir la ley era fundamental para investigar, localizar y enjuiciar a los autores de delitos cibernéticos.

261. El Centro sobre la Delincuencia Transnacional de Filipinas, que es la secretaría de la Oficina Central Nacional de INTERPOL en Manila, y el Consejo de Lucha contra el Blanqueo de Dinero habían acogido conjuntamente la reunión operacional de INTERPOL sobre los fondos robados del Banco de Bangladesh, uno de los mayores casos de blanqueo de dinero.

262. Con respecto a las buenas prácticas en materia de pruebas electrónicas y prácticas delictivas, Filipinas informó de que los organismos especializados utilizaban la ciencia forense digital para localizar, investigar y enjuiciar a los autores de delitos cibernéticos. La Ley de Prevención de la Ciberdelincuencia de 2012, aprobada el 12 de septiembre de 2012, había entrado en vigor el 18 de febrero de 2014. La entrada en vigor de dicha Ley, unida al uso de las normas sobre pruebas electrónicas emitidas por el Tribunal Supremo, había mejorado la eficacia del enjuiciamiento de los casos de ciberdelincuencia en los tribunales competentes en la materia.

263. El 2 de mayo de 2017 el Centro de Investigación y Coordinación sobre Ciberdelincuencia había puesto en marcha el Plan Nacional de Ciberseguridad 2022, en el que se reconocía la urgencia de proteger a todos y cada uno de los usuarios de Internet en Filipinas, la infraestructura nacional de información esencial, las redes gubernamentales, las pequeñas y medianas empresas y otras empresas y sociedades.

264. A pesar de los esfuerzos que estaba realizando el Gobierno para combatir la ciberdelincuencia junto con los organismos especializados, la promulgación de leyes para luchar contra la ciberdelincuencia, la creación de tribunales de ciberdelincuencia y la utilización de normas sobre pruebas electrónicas, seguía siendo necesario impartir capacitación a los especialistas y expertos sobre la utilización de esas herramientas. Se deberían aprovechar las actividades de creación de capacidad que se estaban llevando a cabo en la actualidad, especialmente las que contaban con patrocinios, fueran estos

locales o extranjeros. Además, se deberían realizar periódicamente evaluaciones y valoraciones de la ciberdelincuencia y la ciberseguridad para hacer balance de hacia dónde estaban llevando esas iniciativas a Filipinas.

Portugal

265. Portugal afirmó que las tecnologías de la información y las comunicaciones creaban nuevas oportunidades para los delincuentes y daban lugar a un aumento de la tasa y la diversidad de los delitos cometidos en el mundo digital y por medio de él. Esos delitos repercutían cada vez más en la estabilidad de las infraestructuras vitales de los Estados y las empresas y en el bienestar de las personas, debido a sus consecuencias para el pleno disfrute de los derechos humanos y las libertades civiles. La utilización de las tecnologías y de Internet para difundir contenidos terroristas, para fomentar el discurso de odio y para el extremismo y el radicalismo, así como para cometer otros delitos graves como el abuso sexual de niños, la trata de personas y el blanqueo de dinero, eran algunos ejemplos de las preocupaciones de los Estados en la era digital.

266. Portugal señaló que los Estados se enfrentaban a dificultades en las investigaciones penales debido a la utilización de tecnologías de cifrado, la dificultad para obtener y preservar las pruebas electrónicas, el ejercicio de la jurisdicción en el ciberespacio y la falta de cooperación internacional en ese ámbito. La utilización del cifrado respondía a una necesidad legítima de privacidad y de ejercicio de los derechos fundamentales, así como a las necesidades de las empresas y de las autoridades públicas; las empresas habían invertido en el desarrollo de herramientas que ofrecían una mejor protección de la privacidad de sus clientes, y afirmaban que las iniciativas para debilitar el cifrado podían exponer la información privada a personas que podían usarla de forma indebida. El procesamiento seguro era un elemento importante de la protección de los datos personales y el cifrado estaba reconocido como medida de seguridad en el Reglamento 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea. Sin embargo, además de mantener los datos o la información seguros, las tecnologías de cifrado también ofrecían buenas oportunidades para los delincuentes.

267. Otro desafío para las investigaciones y los enjuiciamientos era el de cómo obtener y conseguir las pruebas electrónicas almacenadas en sistemas informáticos, dada su magnitud y complejidad. Los servicios basados en redes se podían prestar desde cualquier lugar, sin que fuera necesaria la presencia de estructuras físicas, instalaciones o personal en el Estado afectado. En consecuencia, las pruebas pertinentes se almacenaban a menudo en servidores situados fuera del Estado investigador, en una o varias jurisdicciones extranjeras, o incluso en una jurisdicción desconocida, y podían involucrar a proveedores multinacionales de servicios.

268. Debido a la falta de conexión entre las autoridades encargadas de la investigación de las distintas jurisdicciones, para la mayoría de las solicitudes de cooperación judicial se requería un acceso transfronterizo a las pruebas electrónicas, y dichas solicitudes se dirigían a menudo a Estados que acogían un gran número de proveedores de servicios pero que no tenían ninguna relación específica con los procedimientos. La obtención de pruebas a través de la cooperación judicial podía durar períodos largos de tiempo, durante los cuales era posible que dichas pruebas dejaran de estar disponibles. Otra dificultad era que no existía un marco claro para la cooperación con los proveedores de servicios privados y los enfoques de cada país respecto de esa cooperación variaban.

269. Portugal se refirió a la prevención y la lucha contra la incitación al terrorismo y a la difusión de contenidos terroristas, así como al fomento del radicalismo y el extremismo por Internet y otras tecnologías de la información y las comunicaciones, como otros desafíos a los que se enfrentaban los Estados en el plano internacional.

270. La lucha contra los delitos cometidos por medio de las tecnologías de la información y las comunicaciones y contra la ciberdelincuencia era un asunto de interés estratégico para Portugal, que estaba firmemente comprometido con esa lucha. En 1991 se había aprobado una ley relativa a los delitos informáticos (Ley núm. 109/1991), que

había sido revisada en 2009 (Ley núm. 109/2009 (Ley de Ciberdelincuencia)). Se estaba revisando la Estrategia Nacional de Seguridad del Ciberespacio (2015) y en los próximos meses estaba prevista la publicación de una nueva estrategia nacional. La utilización de las tecnologías de la información y las comunicaciones y la ciberdelincuencia se mencionaban entre las cuestiones más importantes tanto en las estrategias antiguas como en las nuevas.

271. Portugal informó además de que se había aprobado una ley sobre la conservación de datos generados o procesados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Esa ley era particularmente importante para la investigación penal de delitos graves como el terrorismo y la delincuencia organizada.

272. Portugal consideraba que para luchar contra la ciberdelincuencia era crucial contar con un marco jurídico nacional adecuado y moderno que proporcionara mecanismos y facultades procesales apropiados y, por lo tanto, permitiera a las autoridades encargadas de hacer cumplir la ley y a los fiscales investigar y recopilar pruebas digitales, respetando al mismo tiempo los derechos y las salvaguardias de los sospechosos y de las víctimas.

273. Portugal había creado dependencias especializadas en sus organismos encargados de hacer cumplir la ley y en la judicatura, a saber: dentro del Ministerio Público Fiscal, en 2011 se había creado la Oficina de Ciberdelincuencia, y dentro de la Policía Judicial se había establecido la Unidad Nacional de Lucha contra la Ciberdelincuencia y los Delitos Tecnológicos, que actuaba y se coordinaba a nivel nacional. El Ministerio Público Fiscal era responsable de las investigaciones penales y la Policía Criminal era la autoridad encargada de hacer cumplir la ley, con competencia exclusiva para investigar los delitos cibernéticos y los delitos cometidos mediante la utilización de las tecnologías de la información y las comunicaciones, bajo la dirección del fiscal encargado, tal como se especificaba en la Ley de Organización de la Investigación Penal (Ley 49/2008). Esta especialización aumentaba la eficacia de las investigaciones y garantizaba la coherencia de las respuestas y la coordinación internacional. La cooperación internacional para la obtención de pruebas de otro país era importante y se debían hacer esfuerzos, especialmente a nivel de las Naciones Unidas, para crear capacidad y aumentar la cooperación.

274. En cuanto a otros desafíos, Portugal señaló que la ciberdelincuencia y la utilización de las tecnologías de la información y las comunicaciones para cometer delitos carecían de límites territoriales; se cometían a escala global. Los servicios de alcance mundial (como los servicios de *webmail*, las redes sociales y los servicios de nube) se utilizaban en todas partes y también se podían usar con fines delictivos dirigidos a víctimas de muchos Estados diferentes. Si bien algunos Estados reconocían la necesidad de agilizar los casos que entrañaban pruebas digitales, otros insistían en la utilización de mecanismos tradicionales como las solicitudes de asistencia judicial recíproca, que no permitían responder de forma oportuna a las necesidades o problemas actuales. Se carecía de reglamentos internacionales exhaustivos y los marcos nacionales ofrecían soluciones diversas; por lo tanto, era necesario un enfoque nuevo.

275. Portugal también mencionó que las partes en el Convenio sobre la Ciberdelincuencia del Consejo de Europa estaban redactando un protocolo adicional al Convenio. Se esperaba que dicho protocolo proporcionara a los organismos encargados de hacer cumplir la ley y a la judicatura una orientación clara sobre el acceso transfronterizo a los datos y mejorara la cooperación oficiosa, el intercambio de información y el funcionamiento de la asistencia judicial recíproca para obtener datos almacenados en otras jurisdicciones, respetando al mismo tiempo plenamente los derechos y las libertades fundamentales.

276. A nivel de la Unión Europea, se estaban negociando un reglamento y una directiva sobre las pruebas electrónicas, que permitirían obtener y recopilar pruebas electrónicas y mejorar la cooperación en ese ámbito.

Qatar

277. Qatar declaró que estaba aumentando el uso indebido de los recursos y las tecnologías de la información, en particular mediante la ciberdelincuencia y la piratería electrónica, lo que afectaba a la seguridad y la estabilidad de los países. Los efectos adversos del uso de los recursos o las tecnologías de la información en el desarrollo, la paz, la estabilidad y los derechos humanos se habían examinado en detalle en varias resoluciones de organismos de las Naciones Unidas. Los delitos cometidos en el mundo digital y su creciente diversidad, así como la utilización de esas tecnologías y medios con fines incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales, afectaban negativamente a la integridad de la infraestructura de los Estados y perjudicaban su seguridad en ese ámbito.

278. Era necesario fortalecer las medidas jurídicas a nivel nacional e internacional para hacer frente a la ciberdelincuencia y proponer medidas nuevas para combatirla, detectarla, investigarla y perseguirla. También era preciso intensificar los esfuerzos internacionales para impedir la utilización de los recursos o las tecnologías de la información con fines delictivos y terroristas. Qatar reafirmó su apoyo al Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético y solicitó su continuidad para mantener la paz y la estabilidad y crear un entorno de tecnología de la información y las comunicaciones abierto, seguro, estable y pacífico.

279. Qatar informó de que procuraba mejorar la seguridad de la información dentro del Estado y alentar la cooperación internacional en la lucha contra la ciberdelincuencia, especialmente porque había sido víctima de la piratería electrónica, utilizada para encubrir la creación de una crisis regional artificial que había dañado gravemente la seguridad y la estabilidad regionales e internacionales. Qatar prestaba atención especial a la elaboración de su legislación y a promover la acción internacional conjunta para prevenir los delitos digitales y localizar y enjuiciar a sus autores.

280. Qatar promulgó la Ley núm. 14 de 2014 para luchar contra la ciberdelincuencia, la cual representaba un gran avance para fortalecer la legislación y los procedimientos nacionales a ese respecto. Dicha Ley contenía capítulos en los que se definía la ciberdelincuencia, por ejemplo los delitos de vulneración de los sistemas, programas y redes de información, el fraude electrónico y la falsificación y los delitos de violación de los derechos de propiedad intelectual. Contenía asimismo disposiciones sobre los procedimientos de investigación, la recopilación de pruebas, las obligaciones de los proveedores de servicios, las obligaciones de los organismos estatales y la cooperación internacional, incluidas la asistencia judicial recíproca y la extradición.

281. Por último, Qatar señaló que la ciberdelincuencia, como nueva forma de delincuencia organizada transnacional, era un problema en auge y en evolución. Requería una respuesta colectiva coordinada y cada vez más firme, basada en el principio del interés común y la responsabilidad compartida. En ese contexto, Qatar trataba de fortalecer su cooperación con la UNODC con miras a crear capacidad nacional, mejorar la seguridad de las redes informáticas y promover la cooperación regional e internacional a fin de crear un entorno cibernético seguro y sólido.

Rumania

282. Rumania declaró que, a medida que la tecnología avanzaba, iba desempeñando un papel importante en una gran variedad de actividades delictivas cuyo impacto e influencia en el entorno en línea eran grandes. El término “ciberdelincuencia” hacía referencia a una gran variedad de amenazas delictivas, como la distribución de programas secuestradores y otros programas maliciosos, el fraude con medios de pago distintos del efectivo y el comercio en línea de material de explotación sexual infantil.

283. Rumania describió los “delitos basados en la cibernética” como aquellos delitos que solo se podían cometer utilizando computadoras, redes informáticas u otras formas de tecnología de la información y las comunicaciones. Los “delitos facilitados por la cibernética” se podían perpetrar tanto en línea como fuera de línea. El papel que

desempeñaba Internet era el de aumentar la escala, el alcance geográfico y la velocidad de esos delitos. La explotación sexual infantil en línea representaba la peor cara de los delitos facilitados por la cibernética. Además, la red oscura albergaba cada vez más foros dedicados específicamente a la producción, el intercambio y la distribución de material de explotación sexual infantil. Por otra parte, Internet ofrecía una gran variedad de funciones, como el intercambio de archivos entre pares y el almacenamiento seguro de datos, que facilitaban estos delitos.

284. Rumania se refirió al fraude con medios de pago distintos del efectivo como otra amenaza muy organizada, muy especializada y en constante evolución, que se adaptaba a las contramedidas y a las nuevas tecnologías. Esa amenaza incluía dos tipos de delitos distintos, a saber: el fraude sin presencia de la tarjeta, que se cometía principalmente en línea, y el fraude con presencia de la tarjeta, que se producía normalmente en establecimientos de venta al por menor y cajeros automáticos. Los delincuentes también se estaban infiltrando en los sistemas operativos de los cajeros automáticos para acceder más fácilmente al dinero en efectivo.

285. Rumania informó de que las plataformas de comercio en línea también se podían utilizar para el comercio de bienes y servicios ilícitos. Los mercados ilícitos en línea, tanto en la Internet visible como en la red oscura, proporcionaban instrumentos, por ejemplo juegos de herramientas para la ciberdelincuencia o documentos falsos, que se podían utilizar para cometer otros delitos.

286. Rumania mencionó que, además, otro producto que se comercializaba habitualmente en línea y que posteriormente se utilizaba para fomentar el fraude eran los datos expuestos. Por lo general, se trataba de datos financieros, como datos de tarjetas de pago o información para el inicio de sesión de cuentas bancarias. En esa categoría se podían incluir también datos que iban desde listas de información personal completa y documentos escaneados hasta listas de correo electrónico e información para el inicio de sesión de cuentas en línea.

287. Rumania afirmó que los delincuentes utilizaban todos los canales de comunicación disponibles, no solo para las comunicaciones internas, sino también para ponerse en contacto con las posibles víctimas, por ejemplo a través de campañas de *phishing* por correo electrónico o por los medios sociales. Los delincuentes también utilizaban aplicaciones seguras y servicios similares para ocultar sus actividades delictivas. El aumento de la utilización por los delincuentes y otros agentes malintencionados de servicios de cifrado constituía un grave obstáculo para la detección, la investigación y la persecución de todo tipo de delitos, en particular el terrorismo.

288. Las nuevas formas de pago, como las criptomonedas y las plataformas bancarias y de pago en línea, ofrecían a los delincuentes fórmulas novedosas para financiar y ampliar sus actividades delictivas. El procesamiento rápido de las transacciones entre varias jurisdicciones y la proliferación de herramientas de cifrado y anonimato eran algunos de los obstáculos más importantes que se afrontaban en las investigaciones financieras. La moneda que más utilizaban los delincuentes para efectuar y recibir pagos relacionados con la ciberdelincuencia era el bitcóin. Esa moneda se aceptaba en la mayoría de tiendas con pago automatizado por tarjeta y mercados de la red oscura, y su utilización para delitos fuera del ciberespacio, como el pago de rescates de secuestros, iba en aumento.

289. Rumania destacó que la ciberdelincuencia en el país había evolucionado de manera similar a otros fenómenos delictivos mundiales, como se describía en los informes de Europol correspondientes al período 2014-2017. Los grupos delictivos procedentes de Rumania se habían mostrado notablemente activos en el ámbito de la ciberdelincuencia. Con el tiempo, Rumania también se había convertido en objetivo de estos delitos. La ciberdelincuencia constituía una amenaza para la seguridad nacional en un sentido amplio, en particular para el sistema financiero.

290. Rumania informó de que había realizado gestiones importantes para adoptar una legislación procesal completa que abarcara diferentes aspectos de los procedimientos penales para la obtención de pruebas electrónicas, de conformidad con las salvaguardias y recursos del estado de derecho, sobre la base del Convenio sobre la Ciberdelincuencia

del Consejo de Europa. Dicho Convenio fue ratificado por Rumania en 2003. La legislación nacional que tipificaba como delito las actividades ilícitas, según lo dispuesto en los artículos 2 a 9 del Convenio, abarcaba una gran variedad de conductas indebidas, lo que permitía a las dependencias especializadas investigar los casos pertinentes. Esas disposiciones seguían siendo aplicables, 15 años después de su promulgación, a las nuevas formas de ciberdelincuencia. Las notas de orientación adoptadas por el Comité del Convenio sobre la Ciberdelincuencia ofrecían indicaciones adicionales sobre los elementos constitutivos de los delitos.

291. Como se informó, en 2004 se había creado la Dirección de Investigación de la Delincuencia Organizada y el Terrorismo, dentro de la Fiscalía del país. Además, dentro de la policía se había establecido la Dirección de Lucha contra la Delincuencia Organizada, como estructura especializada de apoyo a las actividades de la Dirección de Investigación de la Delincuencia Organizada y el Terrorismo. En los últimos cinco años se habían investigado más de 28.800 casos de delitos basados en la cibernética o facilitados por ella.

292. Rumania mencionó un ejemplo de esos delitos, a saber, las actividades de "clonación de tarjetas", cuya finalidad era exponer tarjetas bancarias y que comprendían actividades de grupos delictivos en muchas jurisdicciones distintas (la fabricación de las piezas, el montaje de las piezas y el fraude propiamente dicho). Esas actividades estaban recogidas en el artículo 365 del Código Penal. En cuanto al *modus operandi*, la ingeniería social, el *phishing* personalizado, las múltiples capas de servidores de mando y control y el análisis de vulnerabilidades seguían siendo algunas de las técnicas más utilizadas. Un gran desafío para los organismos encargados de hacer cumplir la ley era el aumento de la utilización de herramientas de código abierto por parte de una gran variedad de agentes, lo que dificultaba atribuir una actividad ilegal a personas o grupos específicos. Los ataques con programas maliciosos estaban recogidos en la legislación nacional en el artículo 207 (chantaje) y en los artículos 362 y 363 del Código Penal.

293. Las tácticas de ingeniería social para cometer fraude (*phishing*, *phishing* personalizado, *phishing* de voz, *phishing* de SMS), así como los ataques de "intermediario" o de "intermediario en el navegador", utilizados principalmente para desviar transferencias de dinero, constituían formas comunes de ciberdelincuencia en Rumania. Estaban tipificadas como delitos en los artículos 325 y 249 del Código Penal (dependiendo del caso concreto, se podían presentar cargos adicionales como el uso indebido de dispositivos o la interferencia de datos). La utilización de la plataforma Cobalt Strike para lanzar ataques contra el sistema bancario se investigaba con arreglo a lo dispuesto en los artículos 360, 362 a 363, 366 y 249 del Código Penal.

294. Las actividades de extracción de criptomonedas y la mayoría de las de extracción de criptomonedas con fines maliciosos se investigaban conforme a los artículos 360 y 366 del Código Penal. Conforme a los mismos artículos del Código Penal se investigaban igualmente las actividades de clonación de tarjetas mediante la inserción de dispositivos en los cajeros automáticos.

295. Por último, Rumania señaló que la creación de un marco jurídico amplio basado en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, así como de instituciones especializadas, habían contribuido a dar respuesta a un problema en constante evolución como era el de la ciberdelincuencia y las pruebas electrónicas. En ese momento era necesario aumentar los recursos, la capacitación y la creación de capacidad. Debatir sobre nuevos tratados internacionales en ese ámbito no sería útil y podría dispersar los esfuerzos.

Federación de Rusia

296. La Federación de Rusia señaló que el problema de la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos se había convertido desde hacía mucho tiempo, en cuanto a dimensiones y alcance, en una amenaza mundial que afectaba a todos los países del mundo sin excepción. En la actualidad, la comunidad mundial no contaba con un enfoque unificado respecto de esta

cuestión. En el plano internacional, la situación se veía agravada por la falta de un marco jurídico internacional amplio para la cooperación, e incluso de una terminología común. A nivel regional, varias organizaciones habían elaborado y adoptado instrumentos sobre la materia, pero su capacidad para hacer frente a esos delitos de manera eficaz seguía siendo insuficiente.

297. La Federación de Rusia afirmó que varios Estados habían promovido el Convenio sobre la Ciberdelincuencia del Consejo de Europa como posible solución. Sin embargo, ese instrumento era inadecuado para hacer frente a las amenazas actuales. El Convenio se había elaborado a finales de la década de 1990 y, por lo tanto, no regulaba muchas de las "invenciones" modernas de los delincuentes. Asimismo, abría la posibilidad a infringir los principios de soberanía de los Estados y de no injerencia en los asuntos internos de otros Estados. Así pues, persistía la amenaza de legitimar el acceso de los servicios especiales de un grupo limitado de países a la recopilación incontrolada de datos personales pertenecientes a usuarios de todo el mundo y continuaba la tendencia establecida por varios Estados a consolidar sus beneficios tecnológicos en el espacio de la información y a mantener la "brecha digital" entre los países desarrollados y los países en desarrollo.

298. La Federación de Rusia subrayó que promovía la formulación de principios y normas universales que fueran compartidos por todas las partes interesadas y que sentaran las bases de una cooperación internacional eficaz en la lucha contra la ciberdelincuencia. Ese instrumento podría ser una convención contra los delitos cometidos mediante la utilización de las tecnologías de la información y las comunicaciones, auspiciada por las Naciones Unidas, que tuviera en cuenta las realidades y los principios actuales de la igualdad soberana y la no injerencia en los asuntos internos de los Estados. El proyecto de convención de las Naciones Unidas sobre cooperación en la lucha contra la ciberdelincuencia elaborado por la Federación de Rusia, que se distribuyó como documento oficial (A/C.3/72/12), podía servir de base para esa labor. La Federación de Rusia consideraba que ese proyecto proporcionaría elementos de reflexión que alimentaran un debate sobre el tema en los principales foros internacionales, fundamentalmente en las Naciones Unidas, y consolidaría y centraría las iniciativas de la comunidad internacional sobre la búsqueda de soluciones prácticas en este ámbito.

299. En opinión de la Federación de Rusia, dado el carácter mundial del fenómeno de los delitos de información, no bastaba con examinar las cuestiones únicamente en el marco del foro de Viena de las Naciones Unidas, a saber, el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético. El mandato del Grupo de Expertos se limitaba a examinar, en su mayor parte, los aspectos técnicos de esta cuestión. En el contexto actual se entendía que la tarea primordial era buscar una solución política y crear consenso.

300. Con este fin, la Federación de Rusia subrayó que se debían aplicar con firmeza las disposiciones de la resolución 73/187 de la Asamblea General, relativa a la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Otra solución era la puesta en marcha de un foro permanente dentro de la Asamblea General en el que se examinaran, sobre la base de un enfoque integrado y equilibrado, todos los aspectos de la cooperación internacional en la lucha contra la ciberdelincuencia, cuya finalidad sería encontrar una solución política y crear consenso, teniendo en cuenta las necesidades urgentes de los Estados en ese ámbito y facilitando el intercambio de las mejores prácticas al respecto. Una de las opciones para dicho foro era la creación de un grupo de trabajo de composición abierta de las Naciones Unidas sobre la ciberdelincuencia que se encargara de elaborar y aplicar los documentos correspondientes de los Estados Miembros.

Arabia Saudita

301. La Arabia Saudita mencionó los obstáculos siguientes en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos:

a) La escasa cooperación de las empresas de plataformas digitales con las autoridades encargadas de hacer cumplir la ley y judiciales de todo el mundo;

b) La ausencia de identidad digital en el mundo virtual y el uso de identificadores y datos fantasma, así como la suplantación de identidad de otras personas en Internet, especialmente en los medios sociales;

c) La disparidad de las legislaciones y leyes penales de los Estados miembros;

d) La falta de coordinación, cooperación y asistencia entre los países en la lucha contra la ciberdelincuencia;

e) Los controles inadecuados sobre la prestación de servicios electrónicos (redes, recursos, entornos de nube, servicios, etc.) en muchos países;

f) La falta en muchos países de sistemas avanzados de información que permitieran la vigilancia de las operaciones sospechosas y la detección de su origen y de quienes se encontraban detrás de ellas;

g) La escasa capacidad humana y técnica de las instituciones públicas y privadas y de los particulares en lo relativo a ciberseguridad;

h) La ausencia de legislación internacional para tipificar como delito y rastrear la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, lo que podría contribuir a las iniciativas internacionales para combatirla;

i) La necesidad de perfeccionar las cualificaciones de las personas en el ámbito de la seguridad de la información mediante programas de capacitación especializada;

j) La multiplicidad y variación entre los países de las legislaciones y las leyes que penalizaban las conductas delictivas en el ámbito de la tecnología de la información;

k) El objetivo único de las plataformas de comercio en línea era obtener beneficios. Además, esas plataformas proporcionaban un terreno fértil para los programas informáticos y las aplicaciones que utilizaban la tecnología para ocultar a los usuarios y cometer delitos cibernéticos;

l) El alcance de los delitos cometidos utilizando la tecnología de la información y su potencial transfronterizo, con una coordinación y comunicación deficientes entre los Estados para hacer frente a esos delitos;

m) La sustitución de las monedas tradicionales por monedas digitales facilitaba a los grupos delictivos la ocultación de muchas de sus transacciones financieras en Internet;

n) La escasa sensibilización sobre el uso seguro y óptimo de la tecnología de la información y de Internet;

o) La necesidad de que la Arabia Saudita participara en la legislación internacional para luchar contra el uso indebido de la tecnología;

p) La necesidad de intensificar la prevención sensibilizando a las comunidades sobre los métodos que utilizaban las bandas de delincuentes que actuaban en Internet.

Serbia

302. Serbia informó de que la organización y la jurisdicción de la Fiscalía Especial para la Delincuencia de Alta Tecnología del país se especificaban en la Ley sobre la Organización y las Competencias de las Autoridades Gubernamentales para Luchar contra la Ciberdelincuencia, que había entrado en vigor el 25 de julio de 2005, y en la

Ley de Modificación de la Ley sobre la Organización y las Competencias de las Autoridades Gubernamentales para Luchar contra la Ciberdelincuencia, que había entrado en vigor el 1 de enero de 2010. En consecuencia, la Fiscalía Especial tenía jurisdicción en el territorio de Serbia para actuar en las causas relacionadas con los delitos mencionados.

303. Serbia se refirió a su marco legislativo y estratégico, que incluía los elementos siguientes:

a) La Ley sobre la Organización y las Competencias de las Autoridades Gubernamentales para Luchar contra la Ciberdelincuencia;

b) La Ley de Confirmación del Convenio sobre la Ciberdelincuencia del Consejo de Europa;

c) La Ley de Confirmación del *Protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*;

d) Ley de Ratificación del Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual;

e) El Código Penal;

f) El Código de Procedimiento Penal;

g) La Ley de Comunicaciones Electrónicas;

h) La Ley de Seguridad de la Información;

i) La Estrategia de Lucha contra la Delincuencia de Alta Tecnología para el Período 2019-2023;

j) La Estrategia para el Desarrollo de la Sociedad de la Información en Serbia hasta 2020;

k) La Evaluación Estratégica de la Seguridad Pública en la República de Serbia.

304. Las reformas recientes de la legislación nacional ponían de relieve la importancia del Convenio sobre la Ciberdelincuencia del Consejo de Europa y su Protocolo Adicional.

305. En septiembre de 2018 el Gobierno había aprobado la Estrategia Nacional de Lucha contra la Ciberdelincuencia y el Plan de Acción correspondiente. Además, el Ministerio de Justicia había creado grupos de trabajo para modificar el Código Penal y el Código de Procedimiento Penal. Con ese fin, en marzo de 2019 representantes de la Fiscalía y de la Fiscalía Especial para la Delincuencia de Alta Tecnología habían iniciado una misión de expertos, dentro del proyecto conjunto iPROCEEDS de la Unión Europea y el Consejo de Europa. Su tarea había consistido en realizar un análisis en profundidad de las lagunas jurídicas de la legislación nacional, evaluando su conformidad con el Convenio sobre la Ciberdelincuencia del Consejo de Europa, la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222 del Consejo, así como con otras normas de la Unión Europea e internacionales. El análisis daría lugar a propuestas para modificar las leyes con el fin de lograr una armonización completa.

306. Serbia indicó que la experiencia de los últimos 15 años demostraba que la creación de capacidad y la especialización a nivel nacional, sobre la base de los acuerdos internacionales existentes, funcionaban muy bien y tenían efectos apreciables. La utilidad de mantener debates sobre nuevos tratados internacionales en ese campo era cuestionable.

307. En relación con el marco institucional y la capacidad administrativa, Serbia enumeró las siguientes instituciones competentes para actuar en el ámbito de la ciberdelincuencia:

a) La Fiscalía Especial para la Delincuencia de Alta Tecnología;

b) El Tribunal Superior de Belgrado;

c) El Departamento de Represión y Lucha contra la Delincuencia de Alta Tecnología del Ministerio del Interior;

d) Otras autoridades estatales competentes.

308. En cuanto a las estadísticas y los análisis, Serbia informó de que, en 2018, el número total de casos inscritos en el registro de la Fiscalía Especial para la Delincuencia de Alta Tecnología había sido 3.022, de los que 322 estaban inscritos en el registro de autores materiales adultos conocidos; se habían registrado 1.306 casos en el registro de autores materiales desconocidos y 1.394 casos en el registro de otros delitos, lo que representaba un aumento del 27,46 % en comparación con 2017.

309. Como consecuencia de lo anterior, se habían observado avances positivos importantes en la aplicación de diversas medidas procesales en distintas etapas de las actuaciones penales, como la presentación de cargos penales contra 324 autores materiales conocidos, lo que representaba un aumento del 28,57 %; la aplicación del enjuiciamiento aplazado había aumentado un 85,71 %, y las negociaciones de los cargos y la condena habían aumentado un 105 %. Las causas de esa subida notable eran el crecimiento del número de personas y casos denunciados, el aumento de los recursos humanos de la Fiscalía Especial y el incremento de la creación de capacidad entre las autoridades competentes.

310. Con respecto a las buenas prácticas, Serbia mencionó los ejemplos siguientes de casos internacionales en los que habían participado autoridades del país especializadas en ciberdelincuencia y que habían llegado a buen puerto gracias a la aplicación del Convenio sobre la Ciberdelincuencia del Consejo de Europa y a las disposiciones sobre cooperación internacional incorporadas a la legislación serbia:

a) La operación “Shadow Web” (febrero de 2018). La desarticulación de “In Fraud”, uno de los mayores foros delictivos, que vendía información de tarjetas de crédito robadas. Se había detenido a un ciudadano serbio y se habían presentado cargos penales;

b) La operación “Power Off” (abril de 2018). El cierre de “Webstresser”, el mayor servicio delictivo de ataques de negación de servicio por contratación del mundo. Se había detenido a dos ciudadanos serbios y se habían presentado cargos penales. Habían participado las autoridades competentes de Alemania, Austria, el Canadá, Croacia, España, los Estados Unidos de América, Italia, los Países Bajos, el Reino Unido y Serbia, así como las de Hong Kong (China). La Fiscalía Especial para Delitos de Alta Tecnología había comenzado a investigar a dos sospechosos y, por primera vez, las autoridades se habían incautado de criptomonedas de un sospechoso;

c) La operación “The Dark Overlord” (mayo de 2018). Esta operación había estado relacionada con un grupo delictivo que había robado datos personales y chantajeado a sus propietarios.

311. Serbia informó de que, en 2018, la cooperación internacional de la Fiscalía Especial había resultado especialmente fructífera. La Oficina había participado en la labor del Grupo contra la Delincuencia Transfronteriza del Convenio sobre la Ciberdelincuencia del Consejo de Europa y en actividades relacionadas con la preparación de nuevas recomendaciones y directrices para la aplicación del Convenio. Asimismo, había intervenido en la labor del grupo encargado de redactar el Segundo Protocolo Adicional al Convenio. La Oficina también había sido incluida en el proyecto conjunto del Consejo de Europa y la Unión Europea GLACY+ y en otras actividades internacionales. En 2018 representantes de la Fiscalía Especial habían tomado parte en el proyecto EAP III del Consejo de Europa, dirigido a lo que se conocía como la “vecindad” de la Unión Europea, y en el proyecto Cyber@South, destinado a los países de África septentrional y occidental y de Asia en el Mediterráneo, así como en el proyecto iPROCEEDS@IPA, en el que se había incluido a países de Europa sudoriental y a Turquía. La Red Judicial Europea sobre Ciberdelincuencia había invitado a la Fiscalía Especial a participar en sus reuniones en La Haya. Representantes de la Fiscalía

Especial también habían participado en la labor del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético.

Singapur

312. Singapur se refirió a los desafíos que enfrentaba, que eran comunes a otras jurisdicciones. Entre esos desafíos se encontraban el perfeccionamiento constante de la sofisticación de los delincuentes, que trataban de aprovecharse del aumento de la accesibilidad derivada de la globalización, y la llegada y la generalización de la tecnología con fines delictivos.

313. Singapur informó de que en el último decenio se había registrado un aumento enorme de la utilización del ciberespacio. Ese auge se había visto alimentado por la reducción de los precios de la tecnología y el aumento de su accesibilidad, lo que había dado lugar a un incremento del número de casos de ciberdelincuencia (delitos tipificados con arreglo a la Ley de Uso Indebido de Computadoras del país y delitos en los que se utilizaran dispositivos o redes informáticas como instrumentos para cometer delitos tradicionales). En ese sentido, el Cuerpo de Policía de Singapur había observado un aumento del número de estafas en línea y cómo las víctimas caían en las tácticas nuevas empleadas por los estafadores internacionales que utilizaban las tecnologías de la información y las comunicaciones, desde métodos de alta calidad como la piratería informática hasta el uso de la tecnología de suplantación de identidad por teléfono. Debido al alcance y la amplitud de los delitos facilitados por la cibernética en todas las jurisdicciones, esos delitos se podían afianzar en cualquier lugar y eran más difíciles de detectar, erradicar y eliminar. Singapur había emprendido iniciativas a nivel nacional, regional e internacional, las cuales se detallaban a continuación, para hacer frente a ese complejo desafío.

314. Con respecto a las iniciativas nacionales, Singapur informó de que el 20 de julio de 2016 el Ministro del Interior y de Derecho había anunciado el Plan de Acción Nacional contra la Ciberdelincuencia de Singapur en la Conferencia RSA para Asia y el Pacífico y el Japón. La visión del Plan de Acción Nacional contra la Ciberdelincuencia era lograr un entorno en línea seguro y fiable para Singapur ante el aumento continuo de la escala, la complejidad y la gravedad de las actividades de los ciberdelincuentes en todo el mundo. En el Plan se detallaba la estrategia multidimensional del Gobierno para luchar contra la ciberdelincuencia a través de las medidas siguientes:

a) Enseñar y capacitar al público para mantener la seguridad en el ciberespacio;

b) Aumentar su capacidad y aptitud para luchar contra la ciberdelincuencia;

c) Fortalecer la legislación y el marco de justicia penal;

d) Reforzar las alianzas y los compromisos internacionales.

315. En cuanto a las iniciativas regionales e internacionales, Singapur señaló la función útil que desempeñaban las organizaciones internacionales y regionales y las alianzas entre múltiples interesados en la creación de capacidad, el fomento de la información, el intercambio de las últimas tendencias y novedades, las mejores prácticas y la cooperación internacional en la lucha contra la ciberdelincuencia transfronteriza.

316. Entre las principales plataformas regionales se encontraban la Reunión de Ministros de la ASEAN sobre la Delincuencia Transnacional y la Reunión de Altos Funcionarios sobre la Delincuencia Transnacional. En su calidad de Coordinador Principal Voluntario de la ASEAN en materia de Ciberdelincuencia, Singapur había introducido iniciativas nuevas para aumentar la capacidad de respuesta de los Estados miembros de la ASEAN contra la ciberdelincuencia, como la celebración de la Conferencia de la ASEAN Más Tres sobre la Ciberdelincuencia y la quinta Mesa Redonda de Altos Funcionarios de la ASEAN sobre la Ciberdelincuencia, en julio de 2018. La ASEAN también había centrado sus esfuerzos en aumentar los conocimientos y la capacidad de los fiscales para enjuiciar los casos de ciberdelincuencia, y en septiembre de 2018 se había celebrado en Singapur la Mesa

Redonda de Fiscales Especializados en Ciberdelincuencia de la ASEAN. Se trataba de eventos anuales que también se organizarían en 2019.

317. Singapur informó de que colaboraba estrechamente con INTERPOL para promover la cooperación regional e internacional en la lucha contra la ciberdelincuencia. El país había sido designado Vicepresidente del Grupo de Trabajo Euroasiático de INTERPOL sobre Ciberdelincuencia entre 2017 y 2019. Además, con el apoyo de INTERPOL, en julio de 2018 había puesto en marcha la Sección de la ASEAN sobre Ciberdelincuencia, en el Complejo Mundial de INTERPOL para la Innovación, situado en el país. Esa Sección de la ASEAN se nutría de los recursos de INTERPOL para impulsar operaciones conjuntas contra la ciberdelincuencia centradas en la ASEAN. Singapur había participado también en la operación Cyber Surge ASEAN, liderada por el Complejo Mundial de INTERPOL para la Innovación, en febrero de 2017. Esa operación había sido todo un éxito, había contado con la participación de siete países de la ASEAN y siete empresas del sector privado, y gracias a ella se habían identificado cerca de 9.000 servidores en situación comprometida y cientos de sitios web infectados con programas maliciosos.

318. Además, Singapur era uno de los asociados de apoyo de INTERPOL World, una conferencia internacional que se celebraba cada dos años en Singapur y en la que los sectores público y privado se reunían para entablar un diálogo y crear oportunidades de colaboración a fin de hacer frente a los desafíos que se iban a plantear en el futuro en los ámbitos de la seguridad y la labor policial. Ese evento singular brindaba a las partes interesadas en la materia una plataforma valiosa para analizar los desafíos de la ciberdelincuencia mundial y recibir información actualizada de expertos sobre las últimas amenazas, tendencias y soluciones.

319. El país había participado asimismo activamente en operaciones internacionales de aplicación de la ley en materia de ciberdelincuencia. Había intervenido en la operación Avalanche, encabezada por la Oficina Federal de Investigación de los Estados Unidos de América, Europol y la Policía Criminal Federal de Alemania, en 2016 y nuevamente en 2017. El objetivo de la operación era desarticular una *botnet* utilizada por una red delictiva para robar información de cuentas bancarias e información de identidad personal con el fin de realizar actividades de blanqueo de dinero, y hacer lo propio con Andromeda, uno de los sistemas de programa malicioso más antiguos que existían. Asimismo, Singapur había participado activamente en plataformas internacionales centradas en intensificar la cooperación mundial y el intercambio de las mejores prácticas en el ámbito de la aplicación de la ley. Entre esas plataformas figuraban la primera Mesa Redonda Nacional de la UNODC sobre Ciberdelincuencia, celebrada en Indonesia los días 2 y 3 de julio de 2018, el Seminario de la UNODC de Expertos en Criptomonedas, que había tenido lugar en Singapur del 12 al 14 de marzo de 2019, así como la reunión del Grupo Mundial de INTERPOL de Expertos en Ciberdelincuencia y la Conferencia INTERPOL-Europol sobre Ciberdelincuencia.

320. Para finalizar, Singapur señaló que los desafíos a los que se enfrentaban los Estados Miembros para luchar contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos tenían múltiples vertientes. La ciberdelincuencia era claramente una cuestión que se vería beneficiada por la continuidad de los debates y el fortalecimiento de la cooperación internacional y de la colaboración a nivel regional e internacional entre los Estados Miembros y las partes interesadas en la materia, y en particular a nivel de las Naciones Unidas. Singapur se había comprometido a respaldar la cooperación internacional y regional contra la ciberdelincuencia y esperaba con interés participar, siempre que fuera posible, en las actividades de creación de capacidad. Además, seguiría apoyando la colaboración y el intercambio de información para enfrentar esos desafíos.

Eslovaquia

321. Eslovaquia informó de que prestaba gran atención a la lucha contra la ciberdelincuencia y consideraba que esa lucha era un desafío importante. Para abordar eficazmente la cuestión de la ciberdelincuencia se debían observar dos aspectos fundamentales: el jurídico y el técnico. En primer lugar, era necesario contar con una legislación nacional adecuada. Las disposiciones sustantivas del derecho penal se debían complementar con disposiciones procesales adecuadas. Para Eslovaquia era importante garantizar que las disposiciones procesales tradicionales, como el registro domiciliario y la entrega, incautación o decomiso de un objeto, se extendieran también a los datos de los medios incautados. Por lo tanto, con respecto al registro de datos informáticos, se necesitaban disposiciones procesales adicionales para poder obtener legalmente los datos informáticos de una manera que fuera tan eficaz como el registro e incautación de soportes de datos tangibles. Sobre esta base, era imprescindible que las legislaciones nacionales contuvieran disposiciones que permitieran a las autoridades del Estado registrar e incautarse de los datos informáticos almacenados. Se debía garantizar que todos los Estados contaran con disposiciones adecuadas para impedir que los autores de los delitos se escondieran para eludir la justicia.

322. Para Eslovaquia, un ejemplo perfecto de modelo que contenía una gran variedad de competencias procesales era el Convenio sobre la Ciberdelincuencia del Consejo de Europa, que recogía, entre otras cosas, disposiciones sobre el registro y la incautación, las órdenes relativas a datos informáticos y la conservación de datos. El país había ratificado ese Convenio en 2008 y consideraba que era la mejor norma internacional, pues contenía disposiciones sustantivas y procesales adecuadas y permitía una cooperación internacional eficaz. A la luz de lo anterior, para Eslovaquia la aplicación con éxito de las facultades procesales contenidas en el Convenio sobre la Ciberdelincuencia del Consejo de Europa y la voluntad política clara eran factores decisivos a fin de disponer de un marco sólido para la obtención de pruebas.

323. Además, Eslovaquia opinaba que la importancia del artículo 18, párrafo 1 a), del Convenio sobre la Ciberdelincuencia del Consejo de Europa, que preveía la emisión de órdenes de presentación, radicaba en que verdaderamente resistía el paso del tiempo. El elemento fundamental no era la ubicación de los datos, sino la presencia de una persona que los controlara o fuera su titular en un territorio específico. Ese enfoque proporcionaba soluciones para la mayoría de los casos, incluso en la era de la computación en la nube. Sobre la base de lo anterior, Eslovaquia no veía la necesidad de elaborar un instrumento internacional nuevo sobre la ciberdelincuencia y alentaba a los países que no eran partes en el Convenio sobre la Ciberdelincuencia del Consejo de Europa a que se adhirieran a él.

324. Eslovaquia señaló además que casi todos los delitos podían generar pruebas electrónicas. El Convenio sobre la Ciberdelincuencia del Consejo de Europa permitía obtener pruebas electrónicas para todos los tipos de delitos, lo que lo convertía en un instrumento más importante aún. De ello se deducía que todos los jueces o fiscales debían estar informados de cómo utilizar los medios disponibles para obtener pruebas electrónicas. A ese respecto, se consideraban esenciales las actividades de capacitación y los programas de creación de capacidad en los planos nacional e internacional. Según Eslovaquia, los programas de creación de capacidad debían ser específicos y, a ser posible, se debía evitar su duplicación.

325. Eslovaquia se refirió asimismo a los aspectos técnicos, además de los jurídicos. Los Estados debían tener presente que un factor decisivo para el éxito de las investigaciones sobre la ciberdelincuencia y los delitos facilitados por la cibernética radicaba en contar con distintos tipos de especialización (redes locales de fiscales, jueces de ciberdelincuencia, autoridades judiciales especializadas en ciberdelincuencia, etc.), así como en la capacitación periódica de las autoridades judiciales y las autoridades encargadas de hacer cumplir la ley, a fin de que las facultades procesales se aplicaran correctamente y dieran respuesta a los acontecimientos actuales. Era necesario crear redes e intercambiar las mejores prácticas dentro de los Estados y a nivel internacional.

326. Para garantizar la especialización y la actualización continua de los conocimientos especializados, Eslovaquia había creado un departamento especializado en ciberdelincuencia dentro del Presidium del Cuerpo de Policía. Ese departamento ayudaba a combatir de manera más eficaz los delitos informáticos y los delitos cometidos a través de Internet. En la actualidad, el departamento se ocupaba principalmente de los ciberataques a los sistemas de información, la explotación sexual infantil en línea, el fraude con medios de pago distintos del efectivo y los contenidos ilícitos en línea (incluidos los contenidos terroristas). Entre sus tareas se incluían el rastreo y la vigilancia de la ciberdelincuencia (incluidas las operaciones encubiertas por Internet). También brindaba cooperación a los fiscales cuando necesitaban asistencia técnica. La cooperación funcionaba muy bien. El departamento se mantenía asimismo en diálogo con la comunidad policial internacional encargada de la ciberdelincuencia, así como con el sector privado, especialmente con los proveedores de servicios de Internet, tanto de Eslovaquia como del extranjero, ya que los datos de las personas solían estar en poder o bajo el control de entidades privadas y era necesario analizar las complejidades y los desafíos de la cooperación.

327. Además, en 2017 se había creado la Red Nacional de Fiscales contra la Ciberdelincuencia. Sus tareas principales eran proporcionar información práctica e intercambiar experiencias entre los miembros de la Red y con otros fiscales encargados de la ciberdelincuencia, tanto en casos nacionales como en casos de cooperación internacional.

328. A nivel nacional se había creado un grupo multidisciplinario de expertos en ciberdelincuencia. En él se reunían expertos de todas las autoridades estatales importantes y del sector privado. Se debatía, entre otras cosas, sobre cómo modificar la legislación relativa a la divulgación de datos en los procedimientos penales para que no fuera necesaria una orden judicial (en Eslovaquia se necesitaba una orden judicial para determinar quién era el usuario de un número de teléfono o de una dirección IP). Por consiguiente, Eslovaquia consideraba que era beneficioso crear redes especializadas a nivel nacional e internacional que reunieran a los profesionales encargados de la ciberdelincuencia.

329. Eslovaquia subrayó que se había comprometido a luchar contra la ciberdelincuencia. Confirmó que, debido al carácter mundial de la ciberdelincuencia, valoraba mucho la posibilidad de participar en el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético. Era muy útil compartir las mejores prácticas e intercambiar opiniones con expertos de todo el mundo en el marco de ese Grupo de Expertos, que debería seguir siendo el proceso principal a nivel de las Naciones Unidas en relación con la cuestión de la ciberdelincuencia, al menos hasta 2021.

Eslovenia

330. Eslovenia reconoció que, con el rápido desarrollo de la tecnología de la información, estaban apareciendo en el mercado nuevos servicios, equipos y dispositivos, junto con nuevos *modus operandi* de los delincuentes. Ante esto, las autoridades encargadas de hacer cumplir la ley se debían adaptar de forma rápida y adecuada, lo que solo se podía garantizar si existía una cooperación eficaz y estrecha con el sector privado y las entidades de investigación. Dicha cooperación implicaba el intercambio seguro y rápido de información, conocimientos especializados, técnicas y métodos de investigación, así como la capacitación continua del personal. Teniendo en cuenta las tendencias, cabía esperar un aumento de los delitos cometidos mediante la utilización de tecnologías de información modernas, digitales y virtuales o de otras tecnologías.

331. La policía eslovena había observado que los autores de delitos en el ciberespacio eran cada vez más expertos en tecnología y estaban mejor organizados; actuaban a nivel internacional y dejaban menos rastros y pruebas utilizables que pudieran facilitar su localización. Todo sucedía muy rápido, el número de víctimas estaba creciendo y se

tardaba mucho más tiempo en restablecer la normalidad. Los rastros que quedaban estaban en formato digital en su mayor parte y, a menudo, estaban dispersos por varios países o continentes, lo que afectaba negativamente a la duración y los resultados de las investigaciones penales. Otro desafío que señaló era la cantidad cada vez mayor de datos que se debían examinar y analizar en cada investigación, así como el hecho de que más fabricantes de dispositivos electrónicos utilizaban por defecto un cifrado de datos seguro. Eso daba a los delincuentes un alto grado de discreción y hacía que la detección y la prevención fueran mucho más difíciles.

332. El desarrollo y el aprovechamiento de los logros tecnológicos generaban unos desafíos para el entorno internacional que solo se podían superar mediante una mayor cooperación y reciprocidad en el desarrollo de nuevas prácticas para prevenir y limitar los riesgos, creando enfoques, instrumentos y mecanismos nuevos y por medio de una acción más recíproca y de más solidaridad en la prevención a nivel operacional. La dispersión internacional de las pruebas y de la actuación de los autores exigiría la introducción de formas nuevas de investigación, una mejor legislación y mejores cualificaciones y equipos.

Sudáfrica

333. Sudáfrica se refirió a los desafíos relacionados con los instrumentos jurídicos y penales existentes para la utilización de las tecnologías de la información y las comunicaciones e informó de que contaba con legislación para combatir los actos de ciberdelincuencia, en la que se incluían el Proyecto de Ley de Ciberdelincuencia (que pronto sería una ley del parlamento), la Ley de Enjuiciamiento Penal, la Ley de Comunicaciones y Transacciones Electrónicas, la Ley de Cooperación Internacional en Asuntos Penales y la Ley de Protección de la Información Personal. Además, declaró que la falta de consenso internacional sobre cuestiones y conceptos fundamentales como la naturaleza y las dimensiones de las amenazas cibernéticas, la legitimidad de los procedimientos y los resultados de los marcos oficiales y la tipificación como ciberdelincuencia de conductas concretas, entre otros, planteaban dificultades para luchar contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Esos desafíos iban más allá de los elementos de definición, que variaban sustancialmente.

334. Sudáfrica aludió también a la coordinación y la cooperación entre los Estados en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. A pesar de que se disponía de varios mecanismos existentes para promover la coordinación y la cooperación, como la asistencia judicial recíproca, los puntos de contacto designados, las obligaciones de los proveedores de servicios de comunicaciones electrónicas y las instituciones financieras, así como la divulgación rápida de los datos sobre el tráfico por parte de diversos proveedores de servicios, los desafíos para hacer frente a la ciberdelincuencia persistían. Se señalaron como importantes los siguientes: proceso prolongado de asistencia judicial recíproca; distintos organismos con mandatos diferentes, lo que dificultaba la coordinación central; y mecanismo de coordinación y aplicación de las medidas propuestas que no contaba con el pleno apoyo de varias partes interesadas. Si bien los instrumentos regionales existentes podían servir para hacer frente a las ciberamenazas, al permitir la cooperación entre los Estados que eran partes en las convenciones, el mayor problema residía en la posibilidad de que no combatieran eficazmente la ciberdelincuencia a nivel mundial, ya que los Estados que no eran partes en la Convención podían no cooperar. La ausencia de una definición de la ciberdelincuencia acordada universalmente suponía un desafío y, por lo tanto, cada país había elaborado su propia definición, lo que había originado problemas en relación con la asistencia judicial recíproca o la cooperación internacional, entre los que se incluían la extradición y el intercambio de pruebas electrónicas. A fin de aplicar de manera efectiva la legislación sobre ciberdelincuencia, y en particular cuando fuera necesario cooperar con otros Estados, era importante velar por que hubiera cierta armonización de la legislación, lo que exigiría un acuerdo sobre la definición de la ciberdelincuencia. Existían varios instrumentos regionales, vinculantes o no

vinculantes, cuyo objetivo era hacer frente a la ciberdelincuencia, pero muchos países tal vez no deseaban ratificar ninguno de los instrumentos regionales existentes debido a sus estructuras políticas, agendas internacionales y circunstancias socioeconómicas.

335. En cuanto a la asistencia técnica, Sudáfrica observó que, si bien existían acuerdos bilaterales y multilaterales (por ejemplo, disposiciones de la Convención contra la Delincuencia Organizada relativas a la asistencia judicial recíproca, la extradición, la transferencia de presos condenados y el decomiso de activos), los acuerdos regionales y continentales parecían sustituirlos en cuanto a funcionalidad. En la mayoría de los casos, la cooperación internacional en relación con la ciberdelincuencia era limitada y no incluía los procedimientos necesarios para, entre otras cosas, conservar las pruebas, poner a disposición los datos sobre el tráfico de forma acelerada o garantizar la disponibilidad de pruebas.

336. Otros desafíos que persistían, en opinión de Sudáfrica, eran las diferentes legislaciones nacionales de los países, que albergaban descripciones distintas de la ciberdelincuencia; los diferentes procedimientos relativos a la cooperación internacional; los procedimientos oficiales entre países que se debían seguir antes de que las pruebas fueran admisibles ante los tribunales; las leyes sobre privacidad; etc.

337. Para Sudáfrica, la falta de estructuras nacionales para coordinar las solicitudes de asistencia recíproca en varios países con facultades al respecto dificultaba la eficacia de la asistencia judicial recíproca. Los diversos instrumentos regionales destinados a combatir la ciberdelincuencia conducían a la fragmentación y a una cooperación entre países basada en silos, y no lograban garantizar una cooperación internacional adecuada. La falta de un instrumento reconocido universalmente a nivel de las Naciones Unidas que se ocupara de la cooperación internacional en materia de ciberdelincuencia era un factor importante que contribuía a la ineficacia de la cooperación internacional en esa esfera.

338. Sudáfrica estaba convencida de que se debía fortalecer la función de la UNODC, y en particular de la Comisión de Prevención del Delito y Justicia Penal, en la creación de capacidad. Era un problema que varias autoridades nacionales carecieran de fondos para impartir capacitación especializada que les permitiera investigar eficazmente los casos complejos de ciberdelincuencia. Asimismo, resultaba difícil retener a los oficiales experimentados y capacitados debido a la demanda del sector privado. Había una ausencia generalizada de programas de capacitación básica e intermedia en las instituciones de capacitación de los funcionarios encargados de hacer cumplir la ley, y los investigadores experimentados rara vez tenían la oportunidad de asistir a cursos o talleres de capacitación avanzada, debido a su carga de trabajo. Incluso con las mejores intenciones y las medidas propuestas, las limitaciones presupuestarias y de capacidad dificultaban la aplicación de dichas medidas, y la capacidad y los recursos disponibles se limitaban a menudo al mandato de un organismo y no se podían utilizar necesariamente para ayudar a otros organismos. Además, no existían marcos o directrices oficiales para la cooperación entre las partes interesadas en el ámbito de la ciberdelincuencia.

España

339. España informó de que la ciberdelincuencia, como consecuencia de la progresiva utilización de las tecnologías de la información y las comunicaciones, era una de las principales amenazas y uno de los retos más importantes para todos los Estados, también debido a la diversificación de las estructuras y métodos empleados por parte de la delincuencia organizada. Los delincuentes aprovechaban las plataformas de comunicación y las nuevas tecnologías para generar nuevos modelos de negocio ilegal como la utilización de la red oscura o *Darknet* como facilitador para cometer otros delitos (como los tráficos de armas, y la moneda falsa), la utilización de programas maliciosos (*malwares*) sofisticados, como los programas secuestradores (*ransomware*), y controladores de infraestructuras bancarias, así como la aparición de “empresarios

criminales individuales” ofertadores de servicios ilícitos. Todo lo anterior constituía un reto para los servidores públicos de seguridad en particular y para la sociedad en general.

340. El rápido crecimiento a nivel mundial en el número de accesos a Internet, junto con el mayor número de dispositivos que se podían conectar a través del mismo traería consigo un mayor número de potenciales víctimas para los ciberdelincuentes. Además, teniendo en cuenta el aumento de la tasa de crecimiento demográfico de los países en desarrollo (principalmente en África) y las estimaciones de crecimiento de ese continente respecto al número de usuarios de Internet, era fácil prever un aumento significativo en la utilización de la red para la comisión de delitos, especialmente de carácter económico. Sin embargo, al igual que los delincuentes aprendían a explotar las nuevas tecnologías e inventar nuevos *modus operandi*, las autoridades policiales también podían hacer uso de la innovación tecnológica y desarrollar nuevas medidas de investigación para contrarrestar la amenaza de la delincuencia organizada y la delincuencia grave.

341. España consideró que la introducción en la legislación nacional de requisitos relativos a las investigaciones encubiertas en la red era una herramienta fundamental en la lucha contra el uso de las tecnologías de la información y las comunicaciones por la delincuencia organizada y la delincuencia grave. Lo mismo ocurría con la utilización progresiva de nuevas tecnologías como el uso de drones, los programas informáticos específicos dirigidos, la introducción en la nube y el acceso rápido a redes sociales.

342. En España la actuación frente a la delincuencia planificada y desarrollada a través de la red y, en general, a través de las tecnologías de la información y las comunicaciones, constituía una de las líneas directrices de la Estrategia de Seguridad Nacional, publicada en diciembre del año 2013 y actualmente en proceso de actualización. En consecuencia, la lucha contra la delincuencia en la red se planteaba como un aspecto más de un objetivo más amplio que era el de hacer que el uso del ciberespacio fuera seguro, a partir de un modelo integrado. Ello incluía la coordinación y cooperación de las administraciones públicas, el sector privado y los ciudadanos y, al tiempo, la integración de las iniciativas internacionales en el ordenamiento jurídico interno e internacional. Dicho planteamiento se había concretado de distintas maneras.

343. En primer lugar, en el ámbito de las reformas legislativas, en 2015 las Leyes Orgánicas 1/2015 y 2/2015 supusieron una importante reforma del Código Penal español, inspirada en la normativa europea (Directiva UE 2013/40 y Directiva UE 2011/93, DM 2008/919/JAI, etc.) y también en el Convenio del Consejo de Europa sobre la Ciberdelincuencia y el Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual. Esos instrumentos incluían la definición de nuevos tipos penales y, como consecuencia de ello, se habían introducido profundas reformas en las disposiciones relacionadas del Código Penal, como las relativas a ataques informáticos, acoso sexual a menores, pornografía infantil, propiedad intelectual, crímenes de odio, fraudes informáticos y delitos de terrorismo. También en el año 2015, por Ley Orgánica 13/2015, se había abordado una profunda reforma de la Ley de Enjuiciamiento Criminal, inspirada en el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Por esa reforma se habían regulado importantes medidas tecnológicas relacionadas con el registro, el almacenamiento y la conservación de datos. Para facilitar la interpretación de esas novedades legislativas, la Fiscalía General del Estado había publicado diversas circulares sobre la materia.

344. En segundo lugar, en relación con las medidas de carácter organizativo, en España todos los Cuerpos Policiales -nacionales y autonómicos- contaban desde hacía más de 20 años con unidades especializadas, altamente cualificadas en investigación tecnológica, con conocimientos y experiencia para luchar eficazmente contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos. Esos conocimientos especializados permitían a las autoridades policiales aprovechar las nuevas tecnologías, como la inteligencia de datos (*big data*), así como los dispositivos conectados a la red e insertados en productos tales como ropa, joyas o calzados para investigar los delitos e identificar a los sospechosos.

345. También el Ministerio Fiscal español había apostado por la especialización en el ámbito de la ciberdelincuencia. Desde el año 2011 la red nacional de fiscales dedicados específicamente a la intervención frente a los ciberdelitos había desplegado por todo el territorio nacional 150 fiscales aproximadamente, en las 50 capitales provinciales y en un buen número de ciudades seleccionadas. Las unidades especializadas, tanto de la Fiscalía como de los Cuerpos Policiales, mantenían un contacto constante con otros organismos con responsabilidad en materia de ciberseguridad, a fin de asegurar una adecuada coordinación en orden a conseguir que el uso del ciberespacio fuera seguro para todos. Entre esos organismos se encontraban la Agencia Española de Protección de Datos, el Centro Nacional de Protección de Infraestructuras Críticas, el Instituto Nacional de Ciberseguridad, el Centro Criptológico Nacional, el Mando Conjunto de Ciberdefensa y también organismos y entidades del sector privado, como entidades bancarias o encargadas de las telecomunicaciones y otros operadores esenciales.

346. Para España era fundamental continuar potenciando la formación de las unidades especializadas en la lucha contra la ciberdelincuencia, así como incrementar sus medios humanos y materiales. La formación de investigadores y operadores jurídicos -jueces y fiscales principalmente- había generado también especial atención en los últimos años, y se planteaba en dos niveles, a saber:

a) Una preparación de carácter genérico sobre conocimientos básicos e imprescindibles que se orientaba a todos los profesionales implicados en la lucha contra la delincuencia;

b) Una formación especializada para las unidades o colectivos que se ocupaban específicamente de la actuación frente a la ciberdelincuencia.

347. España declaró que la cooperación internacional era importante a fin de dar respuesta al desafío común que representaba la ciberdelincuencia para todos los Estados. Algunos ejemplos de la participación del país en las actividades de cooperación internacional eran la participación activa en la Red 24/7 prevista en el artículo 35 del Convenio sobre la Ciberdelincuencia del Consejo de Europa; en la Red Judicial Europea contra la Ciberdelincuencia (EJCN); y en la Red Europea de Fiscales Especialistas en Propiedad Intelectual (EIPPIN). Igualmente, la Fiscalía española impulsaba y participaba en la red iberoamericana de fiscales especialistas (CibeRed).

348. España informó de que era miembro activo del Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa (TC-Y) y de los grupos de trabajo para la preparación de su Segundo Protocolo Adicional orientado a mejorar la cooperación internacional y la colaboración con operadores, proveedores y entidades del sector civil. España participaba en numerosas investigaciones transnacionales, tanto con países europeos como latinoamericanos, en las que se utilizaban técnicas avanzadas de cooperación como equipos conjuntos de investigación. Igualmente intervenía en actividades formativas en otros países, en muchos casos en calidad de formador.

Sri Lanka

349. Sri Lanka destacó su participación activa en el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, que había examinado recientemente los capítulos 5 y 6 del proyecto de estudio exhaustivo sobre el delito cibernético de febrero de 2013. En su próxima reunión, el Grupo de Expertos se centraría en los dos últimos capítulos, 7 y 8 (Cooperación internacional y Prevención).

350. Sri Lanka quiso aclarar la conexión entre la información solicitada en la resolución 73/187 de la Asamblea General y la labor que estaba realizando la UNODC en relación con el proyecto de estudio exhaustivo sobre el delito cibernético, y si se estaba duplicando la labor del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético.

351. En cuanto a la legislación nacional sobre ciberdelincuencia, Sri Lanka informó de que el principal instrumento legislativo en la lucha contra la ciberdelincuencia era la Ley núm. 24 de 2007 de Delitos Informáticos. Además, la Ley núm. 30 de 2006 de

Fraudes con Dispositivos de Pago trataba específicamente sobre la posesión o el uso de dispositivos de pago no autorizados o falsificados.

352. Sri Lanka había pasado a ser Estado parte en el Convenio sobre la Ciberdelincuencia del Consejo de Europa en 2015. Como tal, había mostrado el compromiso firme de armonizar y mejorar la legislación nacional de conformidad con las mejores normas internacionales disponibles que regían la lucha contra la ciberdelincuencia. El país estaba comprometido también a mejorar las técnicas de investigación y a aumentar la capacidad de los funcionarios de justicia penal para adoptar técnicas de aplicación más eficaces.

353. Si bien las disposiciones de derecho sustantivo contenidas en los artículos 3 a 10 de la Ley de Delitos Informáticos se basaban en los artículos 2 a 8 del Convenio sobre la Ciberdelincuencia del Consejo de Europa, el artículo 9 se reflejaba en parte en el artículo 286A de la Ley núm. 22 de 1995 de Modificación del Código Penal. La Ley núm. 36 de 2003 de Propiedad Intelectual se ocupaba de los delitos contemplados en el artículo 10 del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

354. A fin de hacer frente a la evolución de los desafíos que planteaba la ciberdelincuencia, Sri Lanka había emprendido un examen de las medidas nacionales de justicia penal en el ámbito de la seguridad infantil en línea. A raíz de ello, se había aprobado recientemente una modificación de la Disposición Legislativa sobre Publicaciones Obscenas para abordar de forma exhaustiva los delitos relacionados con la pornografía infantil. Mediante esa modificación se introduciría un nuevo capítulo titulado “Pornografía infantil a través del uso de sistemas informáticos”.

355. En lo que respecta a las medidas de aplicación relacionadas con la ciberdelincuencia y las pruebas electrónicas, las disposiciones procesales contenidas en la parte II de la Ley de Delitos Informáticos preveían la interceptación, la recopilación en tiempo real de información básica sobre los abonados y los datos sobre el tráfico y la formulación de solicitudes de conservación. Esas disposiciones estaban sujetas a salvaguardias compatibles con el artículo 15 del Convenio sobre la Ciberdelincuencia del Consejo de Europa[9].

356. Según el artículo 18 de la Ley, para obtener información básica sobre los abonados que estuviera en posesión de los proveedores de servicios, los organismos encargados de hacer cumplir la ley exigían que existiera una orden emitida por un juez. Para la interceptación de las comunicaciones se debía satisfacer un requisito similar. Las órdenes de conservación de datos con arreglo al artículo 19 de la Ley obligaban a toda persona encargada de una computadora o de un sistema de información a conservar los datos si se lo pedían los organismos encargados de hacer cumplir la ley. Sin embargo, la duración estaba limitada a un período de siete días. Para prorrogar el plazo de conservación era obligatorio obtener una orden judicial.

357. La supervisión judicial de esas medidas procesales protegía a los proveedores de servicios frente a solicitudes innecesarias y arbitrarias de los organismos encargados de hacer cumplir la ley, al tiempo que garantizaba que estos ayudaran a los funcionarios encargados de hacer cumplir la ley a luchar eficazmente contra la delincuencia. Esas salvaguardias en la legislación nacional no habían afectado negativamente la eficiencia ni la eficacia de las investigaciones penales. Por otra parte, habían generado más confianza entre las víctimas y las empresas (especialmente los bancos y las organizaciones del sector financiero) para denunciar los incidentes de ciberdelincuencia y, además, habían generado confianza entre los proveedores de servicios de

[9] Con arreglo a la Ley de Delitos Informáticos, las medidas de investigación intrusivas, tales como el registro e incautación de computadoras o la interceptación de una comunicación, están sujetas a una orden judicial por parte de un juez (artículo 18). La Constitución de Sri Lanka reconoce y garantiza varios derechos fundamentales en el capítulo III. Sri Lanka también es parte en varios tratados internacionales de derechos humanos, como el Pacto Internacional de Derechos Económicos, Sociales y Culturales, el Pacto Internacional de Derechos Civiles y Políticos, la Convención sobre los Derechos del Niño y la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes.

telecomunicaciones para cooperar con los organismos encargados de hacer cumplir la ley. Eso se podría considerar una mejor práctica para los países en desarrollo.

358. Dentro de la policía se había creado una unidad especializada en la investigación de la ciberdelincuencia, con dos dependencias provinciales. Esa unidad funcionaba como punto de contacto las 24 horas del día, en el marco del Convenio sobre la Ciberdelincuencia del Consejo de Europa. Recientemente había sido objeto de mejoras y se habían investigado con éxito más de 750 casos gracias a los conocimientos especializados que habían adquirido los funcionarios nacionales mediante las medidas de creación de capacidad que se mencionaban a continuación.

359. Sri Lanka subrayó que la obtención de pruebas electrónicas de proveedores de servicios extranjeros era vital para la investigación y el enjuiciamiento de los delitos cibernéticos. Dado que las pruebas se encontraban en distintas jurisdicciones, era sumamente necesario contar con métodos de investigación más eficaces, junto con medidas de cooperación internacional eficaces. La cooperación internacional en asuntos de justicia penal se regía por la Ley núm. 25 de 2002, de Asistencia Recíproca en Materia Penal. Esta Ley se había incorporado por remisión a la Ley de Delitos Informáticos, y la Ley 25 de 2002 había sido modificada en 2018 por la Ley núm. 24 de 2018, que contenía características del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

360. En cuanto a las medidas de creación de capacidad, se habían desarrollado una serie de programas sobre la ciberdelincuencia y las pruebas electrónicas, que abarcaban el poder judicial, la Fiscalía General y las dependencias policiales, centrados en mejorar los métodos de cumplimiento e investigación. Esos programas se llevaban a cabo en el marco de un proyecto apoyado por la Unión Europea y el Consejo de Europa. Esas medidas de creación de capacidad habían aumentado la capacidad de los funcionarios nacionales encargados de hacer cumplir la ley para adoptar procedimientos operativos estándar más eficaces, basándose en buenas prácticas y experiencias, así como en las enseñanzas extraídas de otros Estados partes en el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

361. Sri Lanka informó de que el Gobierno había adoptado una estrategia global de ciberseguridad en octubre de 2018. A raíz de ello, estaba redactando actualmente legislación sobre ciberseguridad y protección de datos. Al frente de esas iniciativas estaba el Ministerio de Infraestructura Digital y Tecnología de la Información, apoyado por equipos de respuesta a emergencias informáticas, el Organismo de Tecnología de la Información y las Comunicaciones, el Banco Central de Sri Lanka y otros interesados clave. El Ministerio había incluido al sector privado en esa labor, y el Gobierno iba a adoptar un enfoque inclusivo y consultaría a los interesados clave al examinar los nuevos proyectos de ley.

Suiza

362. Suiza señaló que la evolución de las tecnologías de la información y las comunicaciones, si bien ofrecía oportunidades sin precedentes para los particulares, las sociedades, las empresas y el comercio, también planteaba desafíos, en particular en el ámbito de la justicia penal y, por consiguiente, del estado de derecho. Aun cuando la ciberdelincuencia en sentido estricto, es decir, los delitos cometidos a través de sistemas informáticos, incluidos los delitos que dejaban pruebas electrónicas en los sistemas informáticos, estaba evolucionando, y aunque las pruebas de esos delitos se almacenaban cada vez más en servidores situados en jurisdicciones extranjeras, que podían ser múltiples, cambiantes o desconocidas, por ejemplo en la nube, las autoridades encargadas de hacer cumplir la ley estaban limitadas por las fronteras territoriales y debían respetar la soberanía de los Estados.

363. Suiza observó con inquietud la limitada eficacia de la asistencia judicial recíproca para asegurar las pruebas electrónicas volátiles, las situaciones de pérdida de (conocimiento de) la localización de datos y el hecho de que, ante la ausencia de normas

internacionales, los Estados recurrieran cada vez más al acceso transfronterizo unilateral a los datos.

364. Como Estado parte en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, Suiza destacó la importancia de dicho instrumento. Para Suiza, el Convenio facilitaba enormemente la cooperación mediante la armonización de las leyes, el establecimiento de procedimientos y la designación de puntos de contacto. Era necesario facilitar e incrementar la cooperación internacional sobre la base de dicho Convenio.

365. La cuestión de si un proveedor de servicios estaba suficientemente presente en el territorio de un Estado parte u ofrecía un servicio, quedando así sujeto a la jurisdicción de ese Estado, sería decisiva en los años venideros. Esa cuestión sería relevante no solo en términos de derecho penal, sino también de legislación tributaria y de derecho de autor, por ejemplo.

366. Suiza subrayó que las obligaciones de los Estados con arreglo al derecho internacional, en particular el derecho de los derechos humanos, se debían cumplir en todo momento, incluso al regular el ciberespacio y al tipificar, investigar y enjuiciar los delitos cibernéticos. Se debían tener en cuenta los principios de la protección de datos y otras salvaguardias del estado de derecho, en particular al examinar y debatir formas nuevas de cooperación internacional e investigaciones transnacionales.

República Árabe Siria

367. La República Árabe Siria subrayó que la amenaza de la ciberdelincuencia aumentaba día a día a medida que lo hacía el uso de las tecnologías de la información y las comunicaciones por redes delictivas y grupos terroristas para lograr sus objetivos delictivos y terroristas. Ello afectaba la estabilidad de los países, su infraestructura e instituciones, especialmente el tejido social y cultural, el desarrollo económico y el avance del desarrollo. La ampliación de la brecha digital entre los Estados socavaba inevitablemente la capacidad de muchos Estados para prevenir, enjuiciar y combatir esos delitos.

368. Para la República Árabe Siria, no cabía duda del efecto notable que las elevadas tasas de delincuencia y el aumento del número de delitos cometidos en el mundo digital habían tenido en la propagación de los delitos de terrorismo en todo el mundo, especialmente los cometidos por organizaciones terroristas en el Iraq y en la República Árabe Siria. Un espacio digital incontrolado e insondable facilitaba a los terroristas la comisión de todo tipo de delitos, desde el asesinato, la trata de personas, el tráfico de bienes culturales y el saqueo de monumentos y lugares religiosos, hasta la utilización de Internet para el abuso de menores, el secuestro y el reclutamiento de estos para utilizarlos en hostilidades y terrorismo, los actos de racismo y de incitación al odio y las luchas sectarias, étnicas o doctrinarias, así como otras infracciones graves de las leyes, convenciones y resoluciones internacionales pertinentes que exigían una respuesta internacional firme.

369. La República Árabe Siria había adoptado numerosas medidas, incluso mediante el fortalecimiento de los marcos jurídicos, a fin de hacer frente a la amenaza de la ciberdelincuencia y la utilización por grupos terroristas del espacio digital para cometer las formas más atroces de delitos terroristas transnacionales. Al respecto, el Gobierno promulgó el Decreto Legislativo núm. 17 de 2012 sobre la lucha contra la ciberdelincuencia, así como el Código Penal Digital para aumentar la eficacia de la lucha contra los delitos tradicionales que entrañaban el uso de las tecnologías de la información y las comunicaciones. Se había promulgado la Ley núm. 9 de 2018, que incluía la creación de una fiscalía y tribunales especializados en delitos de información y comunicaciones, para sensibilizar sobre la gravedad de ese delito y crear capacidad y proteger a las víctimas en el país.

370. En la aplicación práctica de la legislación, las autoridades competentes se habían enfrentado a muchos problemas y desafíos, ya que ese tipo de delincuencia no tenía

límites y, por lo tanto, las investigaciones criminales eran más complicadas para las autoridades encargadas de hacer cumplir la ley. Entre esos desafíos se incluía el de hacer frente al monopolio de los países desarrollados en la Internet mundial y la politización de la labor y la falta de cooperación en el ámbito del intercambio con las autoridades de la República Árabe Siria de pruebas e información sobre personas que cometían actividades delictivas a través de Internet. Además, la República Árabe Siria informó de que el bloqueo y las medidas coercitivas unilaterales e ilegales que le habían impuesto los Estados Unidos de América y otros países, así como la Unión Europea, que tenían el monopolio de las tecnologías de las comunicaciones, habían limitado el acceso de las autoridades competentes del país a las tecnologías y herramientas necesarias para combatir esas actividades delictivas.

371. Para la República Árabe Siria, los instrumentos jurídicos de derecho penal que se utilizaban actualmente a nivel internacional y regional eran insuficientes para luchar contra la utilización ilegal de las tecnologías de la información y las comunicaciones en operaciones delictivas y terroristas. En la actualidad no existía ninguna convención internacional en ese contexto, salvo el Convenio sobre la Ciberdelincuencia del Consejo de Europa, que no abarcaba la utilización de la tecnología de la información en actos terroristas.

372. A la luz de lo anterior, y a fin de intensificar la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, la República Árabe Siria recomendó que se adoptaran las medidas siguientes:

a) La adhesión estricta de los Estados a sus obligaciones internacionales y la aplicación de las resoluciones del Consejo de Seguridad contra el terrorismo;

b) Promover una cooperación regional e internacional efectiva, en particular mediante el intercambio de información, y desarrollar un mecanismo flexible convenido para intercambiar información y pruebas digitales;

c) Llegar a un acuerdo preliminar entre los Estados Miembros sobre la manera de buscar soluciones en la lucha contra los delitos cometidos mediante la utilización de las tecnologías de la información y las comunicaciones, que permitiera crear un grupo de trabajo de composición abierta de las Naciones Unidas en Nueva York al objeto de lograr la participación en el examen de ese tema de todos los Estados afectados;

d) Elaborar un instrumento jurídico internacional vinculante sobre la cooperación internacional en ese ámbito que fuera compatible con los intereses de los Estados Miembros, teniendo en cuenta que los instrumentos jurídicos de derecho penal existentes no eran suficientes para combatir los delitos relacionados con las tecnologías de la información y las comunicaciones;

e) Salvar la “brecha digital” mediante el abandono por parte de los Estados de su monopolio sobre la tecnología electrónica y sus herramientas, una vez demostrada la incapacidad de proteger así plenamente contra las consecuencias del uso indebido de las tecnologías de la información y las comunicaciones, levantando las restricciones a la transferencia de tecnología y herramientas a todos los países sin discriminación;

f) Fortalecer las medidas de prevención y protección mediante la cooperación y la participación activa de todos los Estados;

g) Acelerar la respuesta a las solicitudes de cooperación internacional, especialmente con el fin de asegurar y mantener las pruebas digitales, y establecer plazos para dicha respuesta;

h) Valorar la posibilidad de crear una plataforma mundial interactiva en línea que incluyera a las autoridades nacionales competentes de todos los Estados Miembros. La plataforma facilitaría el intercambio de información sobre casos de ciberdelincuencia transnacional y ofrecería directrices acerca de la utilización segura de las bases de datos en línea, y proporcionaría además programas especializados para ayudar a prevenir la ciberdelincuencia y la participación en ella, así como otras directrices que garantizaran una respuesta rápida para hacer frente a la complejidad de la tecnología utilizada en esos delitos;

i) Ofrecer asistencia técnica y crear capacidad a nivel nacional a fin de mejorar las aptitudes de las autoridades competentes para hacer frente con eficacia a los desafíos relacionados con la ciberdelincuencia y los asociados con las pruebas digitales, en particular apoyando las iniciativas nacionales encaminadas a desarrollar y emplazar la infraestructura de Internet para mejorar las capacidades en materia de ciberdelincuencia, así como la capacitación y la sensibilización sobre cuestiones técnicas y la digitalización del mantenimiento de registros;

j) Disponer del equipo necesario para obtener pruebas digitales y apoyar la capacitación de un número suficiente de investigadores digitales cualificados y capacitados en técnicas de verificación de la ciberdelincuencia y en la obtención de pruebas digitales conexas;

k) Establecer normas reguladoras vinculantes sobre el uso del espacio digital, teniendo en cuenta el equilibrio entre la libertad en Internet, la privacidad y la seguridad de los Estados, y elaborar marcos para luchar contra el uso indebido del espacio digital. Por ejemplo, someter a vigilancia los sitios de cambio de bitcoines, que se podrían utilizar para blanquear dinero y financiar el terrorismo, y las plataformas de redes sociales que se utilizaban para incitar a cometer delitos;

l) Fortalecer las alianzas entre los organismos gubernamentales competentes y las empresas del sector privado, como los proveedores de servicios de Internet, las redes de telefonía móvil, etc., para poner la información almacenada a disposición de quien la solicite, de conformidad con los controles legales y judiciales, a fin de culminar la investigación de los delitos de información y obtener pruebas.

Tayikistán

373. Tayikistán señaló que la difusión de las tecnologías de la información y las comunicaciones y el desarrollo de la infraestructura de la información habían contribuido a crear la sociedad de la información. Como ponía de manifiesto la práctica en todo el mundo, la era de la información había ampliado los mecanismos de la violencia política, y a los métodos físicos de persuasión se añadían la manipulación de la conciencia y otras formas de influir en la opinión pública por medio de la información.

374. Tayikistán formuló las recomendaciones siguientes:

a) Se debería alentar a los Gobiernos a que proporcionaran a su personal encargado de hacer cumplir la ley información adecuada y capacitación profesional, así como recursos suficientes para investigar de forma eficaz los delitos relacionados con la utilización de Internet y otras tecnologías de la información y las comunicaciones;

b) Los Gobiernos deberían alentar a sus autoridades encargadas de hacer cumplir la ley a adquirir las habilidades especializadas que facilitaran la investigación de la ciberdelincuencia y les permitieran llevar a cabo las investigaciones criminales con éxito;

c) Los Gobiernos deberían actuar colectivamente para garantizar un intercambio eficaz de información a nivel interinstitucional e interregional, eliminar los obstáculos hallados en unos pocos países para la realización de investigaciones sobre ciberdelincuencia e introducir los cambios necesarios en la legislación, las prácticas y los procedimientos, a fin de acelerar el intercambio de información, la tramitación de las solicitudes procedentes de recursos de información diversos y la transferencia de las pruebas digitales;

d) Era necesario organizar periódicamente cursos específicos y garantizar una capacitación profesional adecuada de los empleados de las autoridades encargadas de hacer cumplir la ley en la lucha contra la ciberdelincuencia y la utilización de Internet y otras tecnologías de la información y las comunicaciones;

e) Se necesitaba elaborar y aprobar una convención universal de las Naciones Unidas sobre la cooperación en la lucha contra los delitos relacionados con la utilización de las tecnologías de la información y las comunicaciones, lo que redundaría en interés de todos los Estados Miembros.

Tailandia

375. Tailandia informó de que entre los delitos cibernéticos que más se solían dar en el país se encontraban la piratería informática, el fraude en Internet, la intromisión, el hostigamiento cibernético, la usurpación de identidad en línea, el abuso de menores en línea, los contenidos ofensivos, los códigos malintencionados y los ataques con programas secuestradores. Los delincuentes siempre buscaban lagunas en la tecnología para ocultar su identidad, recurriendo incluso a enfoques innovadores como el uso de monedas de código abierto (criptomonedas) en el sistema de cadena de bloques para blanquear dinero.

376. Tailandia informó asimismo de que en la mayoría de los casos de ciberdelincuencia se planteaba la dificultad de la recopilación de pruebas digitales. Ello se debía a que las pruebas importantes en el enjuiciamiento de los delitos cibernéticos eran los datos sobre el tráfico informático en poder de los proveedores de servicios de Internet y los proveedores de servicios de medios sociales como Facebook, Line, Instagram, WeChat y WhatsApp, que a menudo estaban registrados en países extranjeros y no estaban obligados a prestar asistencia y cooperación de conformidad con la Ley de Delitos Informáticos de Tailandia. Por lo tanto, los organismos encargados de hacer cumplir la ley podrían tener que obtener esas pruebas por la vía oficial de los tratados de asistencia judicial recíproca. Ese proceso llevaba mucho tiempo y podía resultar difícil en la práctica. La información obtenida a través de canales de cooperación oficiosos, aun siendo útil, podía no ser adecuada como prueba ante un tribunal.

377. Además, algunas nuevas tecnologías, como el cifrado, impedían el acceso a los datos. Algunos teléfonos móviles “inteligentes” no se podían desbloquear sin el consentimiento de los propietarios de los dispositivos, lo que impedía el acceso a sus sistemas operativos. Por otra parte, la falta de herramientas y programas forenses digitales, debido a su elevado costo, era un problema común al que se enfrentaban los analistas forenses informáticos; las herramientas libres y los programas informáticos de código abierto tenían una capacidad limitada para el análisis informático forense.

378. Tailandia también informó de que los organismos encargados de hacer cumplir la ley podrían no tener conocimientos suficientes sobre las pruebas digitales y las tecnologías bancarias y financieras modernas. Muchos funcionarios podían carecer de experiencia en la lectura de estados financieros o en la búsqueda de pruebas circunstanciales, en particular mediante técnicas modernas de investigación cibernética. Por lo tanto, era necesario impartir capacitación sobre ciberdelincuencia a los fiscales y otros funcionarios encargados de hacer cumplir la ley y crear una plataforma para intercambiar conocimientos y mejores prácticas.

379. Aunque la Ley de Delitos Informáticos imponía a los proveedores de servicios la obligación de mantener los datos sobre el tráfico y proporcionar la información que les solicitaran las autoridades competentes, algunos proveedores de servicios no siempre cumplían plenamente. Algunos tardaban en presentar los datos solicitados debido a que tenían un gran número de solicitudes. Algunos eran reacios a revelar datos debido a que les preocupaba la privacidad de los clientes.

380. Tailandia subrayó que el creciente uso de las tecnologías de la información y las comunicaciones y, con ello, el acceso de más dispositivos a los servicios de Internet, habían puesto en peligro las infraestructuras vitales de los Estados y las empresas. Aunque esos dispositivos pudieran verse afectados y expuestos en el plano tecnológico, el sistema de información debía permanecer estable y totalmente seguro. Para proteger el sistema era necesario que hubiera colaboración entre todos los organismos competentes y partes interesadas. Igualmente, era difícil definir con claridad la intención de las solicitudes que recibían los proveedores de servicios.

381. En Tailandia, la Ley de Delitos Informáticos B.E.2550 (2007) era la ley principal en lo relativo a la persecución de la ciberdelincuencia. Se utilizaba juntamente con otras leyes que sancionaban delitos relacionados con la ciberdelincuencia, como el Código Penal, la Ley contra la Trata de Personas, la Ley de Estupefacientes, la Ley de Derechos de Autor y la Ley de Prevención y Represión de la Participación en Organizaciones Delictivas Transnacionales. La promulgación de leyes sobre la materia debía ir acompañada de programas de creación de capacidad para los funcionarios a nivel de las operaciones, en particular para los funcionarios encargados de hacer cumplir la ley, así como de mecanismos de coordinación eficaces. Existía una necesidad urgente de aumentar la alfabetización digital de las partes interesadas, así como su sensibilización y comprensión, y de prepararlas para la aplicación de dichas leyes.

382. En relación con la protección de los derechos de las personas, incluidos los niños, Tailandia informó de que quienes se dedicaban a la trata de personas, el ciberacoso y los fraudes en Internet, en particular las estafas, utilizaban las nuevas tecnologías para comunicarse directamente con las personas y ganarse su confianza con fines delictivos. Al mismo tiempo, las ideologías extremas y negativas se difundían cada vez más por Internet. Entre los desafíos principales se incluían los siguientes:

a) La aplicación efectiva de las leyes y reglamentos vigentes;

b) La coordinación entre los organismos competentes, como los funcionarios encargados de hacer cumplir la ley, los operadores financieros y las partes interesadas;

c) La participación de múltiples partes interesadas en la promoción y protección de los derechos de las personas.

383. En opinión de Tailandia, al investigar los delitos conexos se debían tener en cuenta los sentimientos y las circunstancias de las víctimas y, por lo tanto, era necesario un enfoque basado en los derechos humanos específico para cada contexto. Entre las personas que se encontraban en situación de vulnerabilidad, los niños destacaban como blanco del ciberacoso, el hostigamiento cibernético, los juegos en Internet, el sexteo, las imágenes de abusos sexuales de menores, la captación por Internet con fines sexuales y la sextorsión. Se debía prestar atención especial a los sitios de medios sociales como Facebook, Instagram y Twitter.

384. Para finalizar, Tailandia señaló que ningún país podía prevenir y reprimir la ciberdelincuencia por sí solo. Por lo tanto, la cooperación internacional y el diálogo entre los Estados Miembros eran muy importantes. Tailandia había participado en el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, que era la única plataforma que existía a ese respecto. Esperaba que el mandato y la labor del Grupo de Expertos se prorrogaran más allá de 2021.

Turquía

385. Turquía subrayó que las tecnologías de la información y las comunicaciones se utilizaban en una red amplia en la que intervenían los sectores público y privado, las infraestructuras vitales y los particulares, y que se habían extendido de forma considerable tanto a nivel nacional como internacional. Por esa razón, esas tecnologías desempeñaban un papel importante en el crecimiento y el desarrollo sostenibles. Sin embargo, cuanto más se utilizaba la tecnología, más dependía de ella la sociedad, y más sujeta estaba a los riesgos que acarreaba. Las personas, las empresas, las infraestructuras vitales y los Estados se enfrentaban a problemas graves debido a los ciberincidentes. Las deficiencias de seguridad de los sistemas de información y comunicaciones podían hacer que esos sistemas quedaran fuera de servicio o fueran objeto de uso indebido o, a la larga, podían dar lugar a la pérdida de vidas humanas, pérdidas económicas a gran escala, perturbaciones del orden público o riesgos para la seguridad nacional. Por otra parte, el ciberespacio ofrecía ventajas como el anonimato y la capacidad para negar los ataques a las tecnologías de la información y las comunicaciones. Era difícil detectar a los financiadores y organizadores de los

ciberataques reiterados y avanzados contra los sistemas de información. Esa situación dificultaba la lucha contra las amenazas y los atacantes.

386. En este contexto, era esencial no solo la cooperación a nivel nacional, incluidas las partes interesadas, como los sectores público y privado, las universidades, las organizaciones no gubernamentales y los particulares, sino también la cooperación internacional y el intercambio de información. Uno de los objetivos estratégicos principales de la Estrategia y Plan de Acción Nacional de Ciberseguridad era la lucha contra los delitos cibernéticos. A ese respecto, Turquía apoyaba y contribuía a las actividades que se ejecutaban a nivel internacional dentro del concepto de lucha contra la ciberdelincuencia.

387. Turquía había firmado el Convenio sobre la Ciberdelincuencia del Consejo de Europa en 2010. Posteriormente, había incorporado el Convenio a la legislación nacional en 2014 al promulgar la Ley de Aprobación de la Ratificación del Convenio sobre la Ciberdelincuencia. Además, el Código Penal del país regulaba las cuestiones relacionadas con la ciberseguridad.

388. Turquía observó que, con el uso cada vez más generalizado de Internet y el avance constante de las tecnologías de la información y las comunicaciones, el ciberespacio se había convertido en un punto en el que convergía todo, por lo que atraía a muchos tipos de agentes hostiles. Encontrar a los ciberdelincuentes era cada vez más complicado debido a la estructura en capas de Internet y a los servidores intermediarios que se utilizaban para acceder. El uso malintencionado de esas tecnologías proporcionaba los instrumentos necesarios para cometer delitos cibernéticos y un medio de comunicación conveniente para los grupos terroristas. Las organizaciones ilegales utilizaban las tecnologías de la información y las comunicaciones para promover y difundir propaganda, recopilar información, recaudar fondos, reclutar nuevos miembros, orquestar actividades organizadas, intercambiar información y planificar o coordinar actos terroristas. Los grupos terroristas tendían a utilizar aplicaciones y herramientas que ofrecían canales cifrados para comunicarse o planificar o coordinar sus actos hostiles. En esa situación, a las entidades encargadas de hacer cumplir la ley les resultaba difícil descubrir la identidad y las actividades de los terroristas.

389. En opinión de Turquía, el fortalecimiento de la seguridad de la información a nivel mundial y el desarrollo de una cultura de la seguridad en la comunidad internacional eran cuestiones fundamentales para todas las partes interesadas. Asimismo, era importante fortalecer la legislación internacional y mejorar los acuerdos internacionales bilaterales o multilaterales. Al respecto, Turquía consideraba que la formulación de medidas que ayudaran a prevenir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y reforzaran los mecanismos de cooperación internacional en ese ámbito contribuiría a localizar a los terroristas y frustrar sus actividades.

390. Por otra parte, se podía considerar que los contenidos ilegales publicados en Internet constituían un problema grave que planteaba dificultades para garantizar la ciberseguridad. Los ataques malintencionados perpetrados por organizaciones terroristas contra los valores humanitarios comunes y el derecho a vivir en todo el mundo, así como los contenidos que se difundían a través de Internet como instrumentos de propaganda, ponían de relieve la importancia de prevenir la utilización de Internet con fines ilícitos. En ese contexto, la lucha contra los contenidos ilegales en Internet se debía considerar una responsabilidad no solo de los Estados, sino también de las empresas multinacionales de Internet, que eran los agentes principales en la red. Por consiguiente, los agentes de Internet debían actuar en cooperación con los Estados correspondientes para llevar a cabo una prevención minuciosa de las actividades delictivas que efectuaban todas las organizaciones delictivas en sus plataformas.

391. En opinión de Turquía, teniendo en cuenta que todos los grupos terroristas utilizaban el ciberespacio para desarrollar actividades delictivas con motivaciones diversas, era muy necesario que los intermediarios mundiales de Internet respondieran con la mayor rapidez y sensibilidad posibles a las solicitudes de eliminación de contenidos ilegales relacionados con esos grupos terroristas. Era muy importante aplicar

de manera firme y continua las decisiones relativas a la eliminación de contenidos; de lo contrario, el uso malintencionado de Internet por parte de grupos terroristas podría causar daños irreversibles. En ese sentido, la colaboración entre los proveedores de contenidos y los proveedores de alojamiento afectados era vital para que la cooperación fuera plena. El cumplimiento por los proveedores mundiales de las solicitudes de eliminación de contenidos, de conformidad con la legislación nacional e internacional y las órdenes judiciales, contribuiría en gran medida a luchar contra los contenidos ilícitos en las plataformas en línea.

Reino Unido de Gran Bretaña e Irlanda del Norte

392. El Reino Unido declaró que, a los fines de su respuesta, la "utilización de las tecnologías de la información y las comunicaciones con fines delictivos" se debía interpretar como un concepto que se explicaba por sí mismo (y de mayor alcance que la ciberdelincuencia), aunque la formulación amplia de la pregunta no permitía dar una respuesta directa. Los desafíos para abordar la utilización de las tecnologías de la información y las comunicaciones en los delitos se manifestaban de manera muy diversa y compleja en función de varios factores. Entre esos factores se incluían la motivación de los delincuentes, el perfil o las vulnerabilidades correspondientes de las víctimas, el método y los medios tecnológicos que empleaban los delincuentes, en particular los métodos específicos para enmascarar su actividad y, como reflejo de todo lo anterior, si el delito incluía una intromisión en la red o en el sistema o estaba relacionado con contenidos delictivos (por ejemplo, material de explotación sexual infantil).

393. Ante la diversidad existente y teniendo en cuenta la prevalencia de las tecnologías de la información y las comunicaciones en todos los delitos contemporáneos, ya fuera en forma de pruebas digitales o cuando el componente de la tecnología de la información y las comunicaciones representaba un delito por sí mismo, la utilidad del concepto de "utilización de las tecnologías de la información y las comunicaciones con fines delictivos" para la diagnosis era limitada. El Reino Unido había observado que el "factor digital" había sido una realidad durante cierto tiempo en la delincuencia, lo que era un reflejo tanto de la forma en que los delincuentes habían incorporado la utilización de las tecnologías de la información y las comunicaciones para ampliar la escala y las oportunidades de sus delitos, como del aumento progresivo del uso y la dependencia de Internet en todas las sociedades. Por lo tanto, se podía decir que los desafíos resultantes para las entidades encargadas de hacer cumplir la ley no se podían disociar de algunos de los desafíos innumerables y diversos a los que se enfrentaban las sociedades para dar respuesta a muchos de los delitos contemporáneos en general.

394. No obstante estas cuestiones de definición, el Reino Unido se refirió a una serie de desafíos estratégicos que eran universales respecto de la capacidad de los Estados Miembros para investigar y resolver específicamente los delitos con un componente de tecnología de la información y las comunicaciones, a saber:

a) Capacidad o competencias técnicas insuficientes para llevar a cabo investigaciones digitales, especialmente la falta de personal con buen dominio de la tecnología de la información y las comunicaciones, o dificultades para retener a ese personal, en particular en los organismos nacionales encargados de hacer cumplir la ley;

b) La ausencia de leyes sustantivas nacionales en varias jurisdicciones para tipificar como tales los delitos relacionados con la tecnología de la información y las comunicaciones, y que sirvieran de base para la cooperación internacional mediante el reconocimiento recíproco de esos delitos (doble incriminación);

c) La falta de leyes procesales nacionales, con salvaguardias de derechos humanos y regímenes de supervisión adecuados, que permitieran investigar los delitos relacionados con la tecnología de la información y las comunicaciones y la admisibilidad de las pruebas digitales ante los tribunales;

d) Las dificultades para medir la escala y los efectos indirectos de los delitos relacionados con la tecnología de la información y las comunicaciones y los problemas subsiguientes para sensibilizar al público sobre sus daños y alentar la denuncia de esos delitos;

e) Las dificultades para fomentar la sensibilización del público y la adopción de comportamientos de ciberseguridad, o su sensibilización sobre los delitos relacionados con la tecnología de la información y las comunicaciones para reducir su vulnerabilidad a esos delitos o comprender dónde se habían producido hechos delictivos, a fin de denunciarlos;

f) Las dificultades generales derivadas de países que tenían un estado de derecho débil o de jurisdicciones que no cooperaban y que albergaban a los ciberdelincuentes, lo que reflejaba la naturaleza transfronteriza de dichos delitos y el hecho de que se podían cometer sin dejar un rastro físico en los países afectados;

g) Como se señalaba en la Evaluación Estratégica Nacional de 2018 de la Agencia Nacional contra la Delincuencia, los desafíos que planteaban los medios tecnológicos utilizados por los delincuentes para enmascarar más eficazmente sus actividades, entre los que se encontraban el uso de tecnologías como la red oscura, el cifrado, las redes privadas virtuales y las monedas virtuales.

395. En la comunicación escrita que se presentó en la quinta reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, sobre aplicación de la ley e investigaciones, y pruebas electrónicas y justicia penal, se esbozaban algunas de las dificultades antes mencionadas que revestían interés particular para el Reino Unido[10].

396. Aparte de esos dos temas, la escasez de denuncias de delitos basados en la cibernética seguía representando una dificultad especial. El Reino Unido había detectado una brecha conocida entre las experiencias públicas en materia de ciberdelincuencia y la presentación de denuncias al respecto, mediante una comparación de las encuestas públicas y las estadísticas oficiales de presentación de denuncias sobre la delincuencia.

397. El Reino Unido se enfrentaba también a dificultades relacionadas con la falta de cooperación de algunas jurisdicciones. En la Evaluación Estratégica Nacional de 2018, la Agencia Nacional contra la Delincuencia había señalado que los grupos de ciberdelincuencia, muchos de los cuales actuaban a escala internacional y eran de habla rusa, seguían representando una amenaza para los intereses del Reino Unido. En muchos casos, esos grupos tenían su sede física en jurisdicciones que no permitían la extradición de ciudadanos por esos delitos, o de las que no siempre se obtenía cooperación contra los grupos.

398. El Reino Unido consideraba que el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético brindaba una oportunidad única para seguir estudiando soluciones basadas en el consenso a fin de hacer frente a la ciberdelincuencia entre los Estados Miembros. En particular, el carácter de plataforma de expertos del Grupo, y su mandato de examinar sistemáticamente una gran variedad de temas, era ideal para garantizar que en los debates sobre las respuestas a la ciberdelincuencia se tuvieran en cuenta un conjunto amplio de puntos de vista y posibles soluciones. Por consiguiente, el Reino Unido consideraba que era importante velar por que se reconociera que el proceso del Grupo de Expertos era la plataforma principal para debatir sobre la ciberdelincuencia bajo los auspicios de la Comisión de Prevención del Delito y Justicia Penal, de conformidad con el mandato de la Comisión de examinar otras cuestiones relacionadas con la delincuencia. Además, el Reino Unido alentaba a la UNODC y a los Estados Miembros a que aprovecharan plenamente el Grupo de Expertos como plataforma para los debates técnicos de los expertos, a fin de orientar la labor del programa de asistencia técnica de la UNODC sobre la ciberdelincuencia.

[10] Disponible en https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

399. El Reino Unido consideraba asimismo que el Convenio sobre la Ciberdelincuencia del Consejo de Europa era el marco más eficaz para lograr un mayor consenso internacional y armonizar los enfoques sobre la materia. El Convenio contaba con 63 partes y con un amplio consenso en numerosas regiones, y había demostrado ser compatible con diversos marcos jurídicos e institucionales. Por conducto del Comité del Convenio sobre la Ciberdelincuencia, que facilitaba el diálogo entre las partes en el Convenio, este disponía también de sólidos mecanismos para poder tener en cuenta los avances en el ámbito de la ciberdelincuencia y mantenerse al día de las tecnologías y los desafíos nuevos. Por consiguiente, el Reino Unido recomendaba que los Estados Miembros que aún no fueran parte en el Convenio adoptaran medidas para solicitar la adhesión, a condición de que se garantizaran las debidas salvaguardias de los derechos humanos y las leyes procesales nacionales. En los casos en que no existieran ya disposiciones nacionales de ese tipo, el Consejo de Europa contaba con programas de creación de capacidades para la adhesión, por lo que el Reino Unido consideraba que los Estados Miembros deberían colaborar con el Consejo de Europa para determinar la disponibilidad de esos programas de asistencia técnica a tales fines, cuando procediera.

Estados Unidos de América

400. Los Estados Unidos informaron de que se enfrentaban a cuatro desafíos principales, el primero de los cuales era la presión para limitar la contribución de los expertos a la política internacional. Si bien los métodos tradicionales de aplicación de la ley se podían adaptar a la ciberdelincuencia, los desafíos que se planteaban eran complejos y evolucionaban. Por consiguiente, todo debate sobre políticas de las Naciones Unidas en relación con la ciberdelincuencia se debería beneficiar de las aportaciones directas y el asesoramiento de los expertos técnicos. La presión que ejercían algunos Gobiernos para iniciar debates políticos sobre nuevos tratados mundiales, a pesar de la falta de apoyo consensuado a ese enfoque, consumía recursos valiosos y socavaba la capacidad de los expertos para brindar asesoramiento útil sobre la manera de superar los problemas fundamentales a los que se enfrentaban los Estados Miembros al investigar y enjuiciar los delitos cibernéticos. La aportación de los expertos era esencial para comprender cuestiones complejas como las siguientes:

a) La protección de la libertad de expresión;

b) El establecimiento de límites apropiados a la autoridad del Estado;

c) La aplicación efectiva de los marcos y mecanismos existentes;

d) La prestación oportuna de capacitación y asistencia técnica a los países en desarrollo.

401. Este problema había quedado patente durante la aprobación de la resolución 73/187 de la Asamblea General, en la que una votación por partes había abierto nuevos debates políticos en la Asamblea General de una manera que menoscababa la capacidad del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, establecido con arreglo a la resolución 65/230 de la Asamblea General, para cumplir su mandato. La resolución 73/187 entorpecía la labor del Grupo de Expertos al elaborar otro informe antes de que se completara su propio plan de trabajo, y promovía ese informe en un escenario en el que los expertos en la aplicación de la ley no solían participar. Los Estados Miembros deberían respaldar la aportación y la participación de los expertos en la aplicación de la ley y en justicia penal, la industria privada y la sociedad civil en los procesos de formulación de políticas de las Naciones Unidas. Los Estados Miembros también deberían velar por que los debates sobre políticas se organizaran sobre la base del asesoramiento de los expertos nacionales, que se encontraban en la "primera línea" de la lucha contra la ciberdelincuencia.

402. El segundo desafío estaba relacionado con la evolución de la ciberdelincuencia y de las organizaciones delictivas transnacionales. Las organizaciones delictivas transnacionales habían ampliado el alcance de las amenazas de la ciberdelincuencia

aprovechándose de las tecnologías de la información y las comunicaciones, y en particular de la red oscura, no solo para facilitar los ataques sino también para crear mercados en línea de datos robados. Los Estados Miembros estaban adoptando medidas en respuesta, por ejemplo aumentando el número de adhesiones al Convenio sobre la Ciberdelincuencia del Consejo de Europa. Los países de todas las regiones (incluidos los países en desarrollo y los países desarrollados) habían recurrido a ese Convenio a fin de fortalecer sus leyes nacionales y mejorar su capacidad para cooperar con otros países de una manera que limitara también la capacidad de las organizaciones delictivas transnacionales para aprovechar sus infraestructuras nacionales de tecnología de la información y las comunicaciones con fines delictivos.

403. El tercer desafío se refería a cuando la capacidad nacional era limitada y los marcos jurídicos obsoletos. Los Estados Unidos tenían dificultades para colaborar con sus asociados en la persecución de los delitos cibernéticos cuando esos países tenían una capacidad limitada o no habían actualizado sus marcos jurídicos nacionales y sus autoridades de investigación para hacer frente a la ciberdelincuencia. Si bien algunos países se basaban en la legislación penal general, era mejor contar con leyes específicas sobre ciberdelincuencia. A pesar de la ausencia de una definición consensuada de la ciberdelincuencia, sí había un acuerdo general sobre la conducta dolosa, lo que permitía establecer una lista básica de delitos. La comunidad internacional tenía más de una década de experiencia en la redacción de leyes eficaces, modernas y exhaustivas sobre la ciberdelincuencia, en muchos sistemas jurídicos diferentes. Esas leyes se podían redactar de una manera neutra desde el punto de vista tecnológico, evitando así la necesidad de efectuar modificaciones frecuentes. El Convenio sobre la Ciberdelincuencia del Consejo de Europa había sido la fuente principal de inspiración de otros instrumentos y servía como modelo para la legislación nacional de países con tradiciones culturales y jurídicas diversas, incluidos algunos Estados Miembros que no estaban valorando la posibilidad de adherirse. Las gestiones de los Estados Unidos, junto con otros países, para perseguir la ciberdelincuencia tenían más éxito cuando se trabajaba con países que contaban con leyes específicas al respecto.

404. Asimismo, los Estados Unidos tenían dificultades para trabajar con países que habían logrado la aprobación de leyes específicas sobre la ciberdelincuencia, pero que podían tener una capacidad limitada para aplicar su marco jurídico o no habían adoptado medidas para hacerlo en la práctica. Además, los Estados Unidos seguían teniendo serias dificultades para obtener ayuda de algunos Estados Miembros a fin de localizar, detener y enjuiciar a los delincuentes en sus jurisdicciones y para que autorizaran la cooperación internacional de sus autoridades en casos de ciberdelincuencia. Por ejemplo, existía una necesidad urgente de impartir capacitación especializada en pruebas electrónicas para las autoridades de justicia penal. Por esa razón, los Estados Unidos eran donantes del Programa Mundial contra el Delito Cibernético de la UNODC, así como de programas de capacitación auspiciados por la Organización de los Estados Americanos, el Consejo de Europa, la ASEAN y la Comunidad Económica Africana. Los Estados Unidos recomendaban a los Estados Miembros que prestaran más atención a esos programas, en particular los destinados a los países en desarrollo. Los Estados Miembros deberían dar prioridad a prestar asistencia para la reforma legislativa y a la creación de capacidad para que las nuevas leyes se tradujeran en medidas concretas.

405. El cuarto desafío estaba relacionado con las dificultades para obtener pruebas electrónicas. Al igual que otros Estados Miembros, en la lucha contra la ciberdelincuencia los Estados Unidos tenían dificultades con algunas jurisdicciones extranjeras para obtener acceso a las pruebas electrónicas, que se estaban convirtiendo en un elemento omnipresente en las investigaciones de los organismos encargados de hacer cumplir la ley. Concretamente, los Estados Unidos tenían dificultades para recibir ayuda de los Estados Miembros que carecían de la autoridad o la capacidad jurídicas para responder eficazmente a las solicitudes de pruebas electrónicas.

406. A nivel interno, los Estados Unidos tenían dificultades para ejecutar las miles de solicitudes de pruebas electrónicas de otras jurisdicciones, a menudo porque esos países no entendían los requisitos de los Estados Unidos o no proporcionaban información

suficiente para cumplir las normas jurídicas de los Estados Unidos. Las solicitudes incompletas de asistencia judicial recíproca obligaban a las autoridades del país a solicitar aclaraciones e información adicional a los asociados internacionales, lo que retrasaba la respuesta a las solicitudes. Los Estados Miembros se deberían esforzar por subsanar esas deficiencias, dotando a las autoridades centrales y competentes de los recursos y la capacitación suficientes, de conformidad con las obligaciones contraídas de acuerdo con instrumentos como la Convención contra la Delincuencia Organizada. En la UNODC también se estaba trabajando para proporcionar instrumentos nuevos a las autoridades centrales y competentes. Los Estados Unidos recomendaban además que se aumentara la creación de capacidad en los Estados Miembros sobre los requisitos y procedimientos de asistencia judicial recíproca, y en particular que se impartiera capacitación sobre la redacción de solicitudes adecuadas de pruebas electrónicas.

407. Por último, para obtener pruebas electrónicas, los Estados Miembros estaban recurriendo como base jurídica para la cooperación a tratados bilaterales de asistencia judicial recíproca, así como a convenios y convenciones multilaterales como el Convenio sobre la Ciberdelincuencia del Consejo de Europa y la Convención contra la Delincuencia Organizada. Asimismo, más de 80 países participaban activamente en la red de puntos de contacto sobre delincuencia de alta tecnología del Grupo de los Siete, que funcionaba las 24 horas del día, para facilitar la conservación de datos y otras solicitudes. Los Estados Unidos recomendaban a los Estados Miembros que consideraran la posibilidad de adherirse a esos tratados y redes y de utilizarlos en la lucha contra la ciberdelincuencia.

Venezuela (República Bolivariana de)

408. El Gobierno Bolivariano de Venezuela reconoció la creciente utilización de las tecnologías de la información y las comunicaciones y que el rol de la comunidad internacional en el uso de estas podría contribuir al logro de los objetivos de desarrollo acordados internacionalmente, incluidos los que figuraban en la Agenda 2030 para el Desarrollo Sostenible, y a abordar nuevos desafíos.

409. La República Bolivariana de Venezuela subrayó la importancia de eliminar las barreras para aminorar las brechas digitales, en particular aquellas que dificultaban el pleno logro del desarrollo económico, social y cultural de los países y el bienestar de su población, en particular, en los países en desarrollo. Insistió en que se pusiera fin al uso de las tecnologías de la información y las comunicaciones, incluidas las redes sociales, en contravención del derecho internacional y en detrimento de los intereses de los Estados Miembros.

410. La República Bolivariana de Venezuela alentó el trabajo mancomunado de la comunidad internacional para asegurar el acceso a la sociedad de la información y estimuló el respeto por la igualdad de género y el empoderamiento de las mujeres, la identidad cultural, la diversidad cultural, étnica y lingüística, las tradiciones y las religiones y los valores éticos.

411. La República Bolivariana de Venezuela informó de que apuntaba al uso y tratamiento responsable de la información por parte de los medios de comunicación, de acuerdo con los códigos de conducta y la ética profesional. Los medios en todas sus formas tenían un papel importante en la sociedad de la información y las tecnologías de la información y las comunicaciones debían desempeñar un papel de apoyo en ese sentido. El Gobierno Bolivariano de Venezuela reafirmó la necesidad de reducir los desequilibrios internacionales que afectaban a los medios de comunicación, especialmente en lo que respectaba a la infraestructura, los recursos técnicos y el desarrollo de habilidades humanas.

412. Para la República Bolivariana de Venezuela resultaba preocupante el uso de los medios de comunicación como herramienta para la propaganda hostil contra los países en desarrollo con el objetivo de socavar a sus Gobiernos. A ese respecto, el Gobierno Bolivariano de Venezuela destacó la necesidad de promover medios de comunicación y

fuentes de comunicación alternativos, libres, pluralistas y responsables que reflejaran las realidades e intereses de los países y los pueblos del mundo en desarrollo.

413. En ese sentido, y conscientes de que en la actualidad los instrumentos internacionales de derecho penal para contrarrestar los delitos relacionados con las tecnologías de la información y las comunicaciones eran insuficientes, la República Bolivariana de Venezuela consideró necesaria la creación de una convención de las Naciones Unidas sobre cooperación en esa materia, aprobada y basada en el consenso de la comunidad internacional, que exhortara a todos los Estados Miembros a construir una sociedad de la información responsable y que coadyuvara en la toma de medidas para evitar y abstenerse de cualquier medida unilateral que no estuviera de acuerdo con el derecho internacional y la Carta de las Naciones Unidas y que impidiera el pleno desarrollo económico y social de la población de los países afectados, lo que dificultaba el bienestar de la misma.

414. Esa preocupación por el uso potencial de las tecnologías de la información y las comunicaciones en conflictos internacionales, operaciones encubiertas e ilegales y ataques a terceros países por parte de individuos, organizaciones y Estados mediante el uso de sistemas informáticos de otras naciones, hacía necesario que se tomaran medidas en el seno de las Naciones Unidas para lograr avanzar en la concreción de un documento que ayudara a regular el uso y la cooperación en esa materia.

415. En vista de la preocupación que generaba la capacidad expresada por algunos Gobiernos para responder a tales ataques con armas convencionales, la República Bolivariana de Venezuela reiteró que la forma más efectiva de prevenir y abordar esas nuevas amenazas era a través de la cooperación conjunta entre todos los Estados, que permitiría evitar la conversión del ciberespacio en un teatro de operaciones militares. El Gobierno Bolivariano de Venezuela consideró prioritario promover el diálogo y la discusión permanente entre los Estados Miembros a fin de compartir las buenas prácticas y experiencias nacionales o regionales, con especial atención a los países en desarrollo. Asimismo, acompañó la propuesta de creación de un grupo intergubernamental de trabajo, bajo los lineamientos de las Naciones Unidas, para la búsqueda de soluciones y la resolución de diferencias basándose en la igualdad de los Estados.

416. La República Bolivariana de Venezuela reconoció además que el uso ilícito de las tecnologías de la información y las comunicaciones podría tener un impacto perjudicial en la infraestructura, la seguridad nacional y el desarrollo económico de un Estado Miembro, por lo que puso énfasis en la necesidad de aumentar los esfuerzos internacionales para abordar ese problema.